CIS Microsoft Office 365 ProPlus STIG Benchmark

v1.0.0 - 09-11-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Microsoft Office 365 ProPlus Security Technical Implementation Guide Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Office 365 ProPlus Security Technical Implementation Guide and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Microsoft Office 365 ProPlus Security Technical Implementation Guide.

Recommendations

1 STIG RULES

Microsoft Office Enterprise

Microsoft Office 365 ProPlus Security Technical Implementation Guide Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 O365-AC-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Macros must be blocked from running in Access files from the Internet.

```
GROUP ID: V-223280
RULE ID: SV-223280r961050
```

Rationale:

This policy setting allows you to block macros from running in Office files that come from the Internet.

If you enable this policy setting, macros are blocked from running, even if “Enable all macros” is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to “Enable Content”, users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

If you disable or do not configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Access 2016 >> Application Settings >> Security >> Trust Center "Block macros from running in Office files from the Internet" is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\access\security

If the value blockcontentexecutionfrominternet is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Access 2016 >> Application Settings >> Security >> Trust Center "Block macros from running in Office files from the Internet" to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.2 O365-AC-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Trust Bar Notifications for unsigned application add-ins in Access must be disabled and blocked.

```
GROUP ID: V-223281
RULE ID: SV-223281r1016166
```

Rationale:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if the "Require that application add-ins are signed by Trusted Publisher" policy setting is enabled, which prevents users from changing this policy setting.

If users enable this policy setting, applications automatically disable unsigned add-ins without informing users.

If this policy setting is disabled, if this application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If users do not configure this policy setting, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Access 2016 >> Application Settings >> Security >> Trust Center "Disable Trust Bar Notification for unsigned application add-ins and block them" is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\access\security

If the value NoTBPromptUnsignedAddin is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Access 2016 >> Application Settings >> Security >> Trust Center "Disable Trust Bar Notification for unsigned application add-ins and block them" to "Enabled".

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.3 O365-AC-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VBA macros not digitally signed must be blocked in Access.

```
GROUP ID: V-223282
RULE ID: SV-223282r1082349
```

Rationale:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If this policy setting is enabled, choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office. This option also allows users to potentially enable unsigned/untrusted macros. If a site requires the use of macros, they must be signed/approved and added to appropriate locations listed in the Trust Center Settings.
- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.
- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.
- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

If this policy setting is disabled, "Disable all with notification" will be the default setting.

If this policy setting is not configured, when users open files in the specified applications that contain VBA macros, the applications open the files with the macros disabled and display the Trust Bar with a warning that macros are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content", then the document is added as a trusted document.

Important: If "Disable all except digitally signed macros" is selected, users will not be able to open unsigned Access databases.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Access 2016 >> Application Settings >> Security >> Trust Center >> VBA Macro Notification Settings is set to "Disable all except digitally signed macros".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\access\security

If the value vbawarnings is REG_DWORD = 3, this is not a finding. A value of REG_DWORD = 2 or REG_DWORD = 4 is also acceptable. If the registry key does not exist, or is not configured properly, this is a finding.

Remediation:

Set User Configuration >> Administrative Templates >> Microsoft Access 2016 >> Application Settings >> Security >> Trust Center >> VBA Macro Notification Settings to "Disable all except digitally signed macros".

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.4 O365-CO-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Macro Runtime Scan Scope must be enabled for all documents.

```
GROUP ID: V-223284
RULE ID: SV-223284r961092
```

Rationale:

This policy setting specifies for which documents the VBA Runtime Scan feature is enabled.

If the feature is disabled for all documents, no runtime scanning of enabled macros will be performed.

If the feature is enabled for low trust documents, the feature will be enabled for all documents for which macros are enabled except:

- Documents opened while macro security settings are set to "Enable All Macros"
- Documents opened from a Trusted Location
- Documents that are Trusted Documents
- Documents that contain VBA that is digitally signed by a Trusted Publisher

If the feature is enabled for all documents, then the above class of documents are not excluded from the behavior.

This protocol allows the VBA runtime to report to the Anti-Virus system certain high-risk code behaviors it is about to execute and allows the Anti-Virus to report back to the process if the sequence of observed behaviors indicates likely malicious activity so the Office application can take appropriate action.

When this feature is enabled, affected VBA projects' runtime performance may be reduced.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016>> Security Settings "Macro Runtime Scan Scope" is set to "Enable for all documents".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\common\security

If the value for macroruntimescanscope is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016>> Security Settings "Macro Runtime Scan Scope" to "Enable for all documents".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.5 O365-CO-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Document metadata for rights managed Office Open XML files must be protected.

```
GROUP ID: V-223285
RULE ID: SV-223285r1067544
```

Rationale:

This policy setting determines whether metadata is encrypted in Office Open XML files that are protected by Information Rights Management (IRM). If this policy setting is enabled, Excel, PowerPoint, and Word encrypt metadata stored in rights-managed Office Open XML files and override any configuration changes on users' computers.

If this policy setting is enabled, Office 2016 applications cannot encrypt metadata in rights-managed Office Open XML files, which can reduce security. If this policy setting is not configured when Information Rights Management (IRM) is used to restrict access to an Office Open XML document, any metadata associated with the document is not encrypted.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Protect document metadata for rights managed Office Open XML Files" is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\common\security

If the value DRMEncryptProperty is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Protect document metadata for rights managed Office Open XML Files" to "Enabled".

Additional Information:

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

1.6 O365-CO-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Office client must be prevented from polling the SharePoint Server for published links.

```
GROUP ID: V-223286
RULE ID: SV-223286r960963
```

Rationale:

This policy setting controls whether Office 365 ProPlus applications can poll Office servers to retrieve lists of published links.

If this policy setting is enabled, Office 365 ProPlus applications cannot poll an Office server for published links.

If this policy setting is disabled or not configured, users of Office 365 ProPlus applications can see and use links to Microsoft SharePoint Server sites from those applications. Published links can be configured to Office applications during initial deployment, and can add or change links as part of regular operations. These links appear on the My SharePoint Sites tab of the Open, Save, and Save As dialog boxes when opening and saving documents from these applications. Links can be targeted so they only appear to users who are members of particular audiences.

Note: This policy setting applies to Microsoft SharePoint Server specifically. It does not apply to Microsoft SharePoint Foundation.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Server Settings >> Disable the Office client from polling the SharePoint Server for published links is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\common\portal

If the value for linkpublishingdisabled is REG_DWORD = "1", this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Server Settings >> Disable the Office client from polling the SharePoint Server for published links to "Enabled".

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.7 O365-CO-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Custom user interface (UI) code must be blocked from loading in all Office applications.

```
GROUP ID: V-223287
RULE ID: SV-223287r961863
```

Rationale:

This policy setting controls whether Office 365 ProPlus applications load any custom user interface (UI) code included with a document or template. Office 365 ProPlus allows developers to extend the UI with customization code that is included in a document or template.

If this policy setting is enabled, Office 365 ProPlus applications cannot load any UI customization code included with documents and templates.

If this policy setting is not configured or disabled, Office 365 ProPlus applications load any UI customization code included with a document or template when opening it.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Global Options >> Customize >> Disable UI extending from documents and templates is set to Enabled: Disallow in Word; Excel; PowerPoint; Access; Outlook; Publisher; Project; Visio; InfoPath

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\common\toolbars

If the value noextensibilitycustomizationfromdocument is REG_DWORD = 1 for all installed Office programs, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Global Options >> Customize >> Disable UI extending from documents and templates to Enabled: Disallow in Word; Excel; PowerPoint; Access; Outlook; Publisher; Project; Visio; InfoPath.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b

- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.8 O365-CO-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

ActiveX Controls must be initialized in Safe Mode.

```
GROUP ID: V-223288
RULE ID: SV-223288r961779
```

Rationale:

This policy setting specifies the Microsoft ActiveX initialization security level for all Microsoft Office applications. ActiveX controls can adversely affect a computer directly. In addition, malicious code can be used to compromise an ActiveX control and attack a computer.

To indicate the safety of an ActiveX control, developers can denote them as Safe for Initialization (SFI). SFI indicates that a control is safe to open and run, and that it is not capable of causing a problem for any computer, regardless of whether it has persisted data values or not. If a control is not marked SFI, it is possible that the control could adversely affect a computer--or it could mean that the developers did not test the control in all situations and are not sure whether it might be compromised in the future. If you enable this policy setting, you can set the ActiveX security level to a number between 1 and 6. These security levels are as follows:

1. Regardless of how the control is marked, load it and use the persisted values (if any). This setting does not prompt the user.
2. If SFI, load the control in safe mode and use persisted values (if any). If not SFI, load in unsafe mode with persisted values (if any), or use the default (first-time initialization) settings. This level is similar to the default configuration, but does not prompt the user.
3. If SFI, load the control in unsafe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with default (first-time initialization) settings.
4. If SFI, load the control in safe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with default (first-time initialization) settings.
5. If SFI, load the control in unsafe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with persisted values.

6. If SFI, load the control in safe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with persisted values.

If you disable or do not configure this policy setting, if a control is marked SFI, the application loads the control in safe mode and uses persisted values (if any). If the control is not marked SFI, the application loads the control in unsafe mode with persisted values (if any), or uses the default (first-time initialization) settings. In both situations, the Message Bar informs users that the controls have been disabled and prompts them to respond.

Important: Some ActiveX controls do not respect the safe mode registry setting, and therefore might load persisted data even though you configure this setting to instruct the control to use safe mode. This setting only increases security for ActiveX controls that are accurately marked as SFI. In situations that involve malicious or poorly designed code, an ActiveX control might be inaccurately marked as SFI.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "ActiveX Control Initialization" is set to "Enabled (If SFI, load the control in safe mode and use persisted values (if any). If not SFI, prompt the user and advise them that it is marked unsafe. If the user chooses No at the prompt, do not load the control. Otherwise, load it with persisted values.)

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\Common\Security

If the value UFIControls is set to REG_DWORD=6, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "ActiveX Control Initialization" to "Enabled + 6".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.9 O365-CO-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Macros in all Office applications that are opened programmatically by another application must be opened based upon macro security level.

```
GROUP ID: V-223289
RULE ID: SV-223289r961092
```

Rationale:

This policy setting controls whether macros can run in an Office 365 ProPlus application that is opened programmatically by another application. If this policy setting is enabled, the user can choose from three options for controlling macro behavior in Excel, PowerPoint, and Word when the application is opened programmatically:

- Disable macros by default ¬- all macros are disabled in the programmatically opened application.
- Macros enabled (default) - macros can run in the programmatically opened application. This option enforces the default configuration in Excel, PowerPoint, and Word.
- User application macro security level - macro functionality is determined by the setting in the "Macro Settings" section of the Trust Center.

If this policy setting is disabled or not configured, when a separate program is used to launch Microsoft Excel, PowerPoint, or Word programmatically, any macros can run in the programmatically opened application without being blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Automation Security" is set to "Enabled (Use application macro security level)".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\Common\Security

If the value AutomationSecurity is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Automation Security" to "Enabled (Use application macro security level)".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.10 O365-CO-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Trust Bar notifications must be configured to display information in the Message Bar about the content that has been automatically blocked.

```
GROUP ID: V-223290
RULE ID: SV-223290r1016167
```

Rationale:

This policy setting controls whether Office 365 ProPlus applications notify users when potentially unsafe features or content are detected, or whether such features or content are silently disabled without notification.

The Message Bar in Office 365 ProPlus applications is used to identify security issues, such as unsigned macros or potentially unsafe add-ins. When such issues are detected, the application disables the unsafe feature or content and displays the Message Bar at the top of the active window. The Message Bar informs the users about the nature of the security issue and, in some cases, provides the users with an option to enable the potentially unsafe feature or content, which could harm the user's computer.

If this policy setting is enabled, Office 365 ProPlus applications do not display information in the Message Bar about potentially unsafe content that has been detected or has automatically been blocked.

Audit:

Verify the policy value for User Configuration >> Microsoft Office 2016 >> Security Settings >> Disable all Trust Bar notifications for security issues is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\common\trustcenter

If the value trustbar is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Disable all Trust Bar notifications for security issues" to "Disabled".

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.11 O365-CO-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Office applications must be configured to specify encryption type in password-protected Office 97-2003 files.

```
GROUP ID: V-223291
RULE ID: SV-223291r961128
```

Rationale:

This policy setting enables you to specify an encryption type for password-protected Office 97-2003 files.

If you enable this policy setting, you can specify the type of encryption that Office applications will use to encrypt password-protected files in the older Office 97-2003 file formats. The chosen encryption type must have a corresponding cryptographic service provider (CSP) installed on the computer that encrypts the file. See the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ registry key for a list of CSPs installed on the local computer. Specify the encryption type to use by entering it in the provided text box in the following form:

<Encryption Provider>,<Encryption Algorithm>,<Encryption Key Length>. For example, Microsoft Enhanced Cryptographic Provider v1.0,RC4,128

If you do not configure this policy setting, Excel, PowerPoint, and Word use Office 97/2000 Compatible encryption, a proprietary encryption method, to encrypt password-protected Office 97-2003 files.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings >> Encryption type for password protected Office 97-2003 files is set to Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256.

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\common\security

If the value defaultencryption12 is set to REG_SZ = "Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256", this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings >> Encryption type for password protected Office 97-2003 files to Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256.

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.12 O365-CO-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Office applications must be configured to specify encryption type in password-protected Office Open XML files.

```
GROUP ID: V-223292
RULE ID: SV-223292r961128
```

Rationale:

This policy setting allows you to specify an encryption type for Office Open XML files.

If you enable this policy setting, you can specify the type of encryption that Office applications use to encrypt password-protected files in the Office Open XML file formats used by Excel, PowerPoint, and Word. The chosen encryption type must have a corresponding cryptographic service provider (CSP) installed on the computer that encrypts the file. See the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ registry key for a list of CSPs installed on the local computer. Specify the encryption type to use by entering it in the provided text box in the following form:

<Encryption Provider>,<Encryption Algorithm>,<Encryption Key Length>

For example: Microsoft Enhanced Cryptographic Provider v1.0,RC4,128

If you disable or do not configure this policy setting, the default CSP is used. The default cryptographic service provider (CSP) is Microsoft Enhanced RSA and AES Cryptographic Provider, AES-128, 128-bit.

Note: This policy setting does not take effect unless the registry key HKEY_CURRENT_USER\Software\Microsoft\Office\16.0<office application name>\Security\Crypto\CompatMode is set to 0. By default the CompatMode registry key is set to 1.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings >> Encryption type for password protected Office Open XML files is set to Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256.

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\common\security

If the value OpenXMLEncryption is REG_SZ = "Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256", this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings >> Encryption type for password protected Office Open XML files to Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256.

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.13 O365-CO-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Users must be prevented from creating new trusted locations in the Trust Center.

```
GROUP ID: V-223293
RULE ID: SV-223293r961353
```

Rationale:

This policy setting controls whether trusted locations can be defined by users, the Office Customization Tool (OCT), and Group Policy, or if they must be defined by Group Policy alone.

If you enable this policy setting, users can specify any location as a trusted location, and a computer can have a combination of user-created, OCT-created, and Group Policy-created trusted locations.

If you disable this policy setting, all trusted locations that are not created by Group Policy are disabled and users cannot create new trusted locations in the Trust Center.

If you do not configure this policy setting, the behavior is the equivalent of setting the policy to Enabled.

Note: InfoPath and Outlook do not recognize trusted locations, and therefore are unaffected by this policy setting.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016\Security Settings\Trust Center >> Allow mix of policy and user locations is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\common\security\trusted locations

If the value for allow user locations is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings >> Trust Center >> Allow mix of policy and user locations to "Disabled".

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

1.14 O365-CO-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Office applications must not load XML expansion packs with Smart Documents.

```
GROUP ID: V-223294
RULE ID: SV-223294r961863
```

Rationale:

This policy setting controls whether Office 365 ProPlus applications can load an XML expansion pack manifest file with a Smart Document.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Smart Documents (Word, Excel) >> Disable Smart Document's use of manifests is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\common\smart tag

If the value for neverloadmanifests is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Smart Documents (Word, Excel) >> Disable Smart Document's use of manifests to "Enabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.15 O365-CO-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The load of controls in Forms3 must be blocked.

```
GROUP ID: V-223295
RULE ID: SV-223295r961086
```

Rationale:

This policy setting allows the user to control how ActiveX controls in UserForms should be initialized based upon whether they are Safe for Initialization (SFI) or Unsafe for Initialization (UFI).

ActiveX controls are Component Object Model (COM) objects and have unrestricted access to users' computers. ActiveX controls can access the local file system and change the registry settings of the operating system. If a malicious user repurposes an ActiveX control to take over a user's computer, the effect could be significant. To help improve security, ActiveX developers can mark controls as SFI, which means that the developer states that the controls are safe to open and run and not capable of causing harm to any computers. If a control is not marked SFI, the control could adversely affect a computer, or the developers may not have tested the control in all situations and are not sure whether their control might be compromised at some future date. SFI controls run in safe mode, which limits their access to the computer. For example, a worksheet control can both read and write files when it is in unsafe mode, but perhaps only read from files when it is in safe mode. This functionality allows the control to be used in very powerful ways when safety was not important, but the control would still be safe for use in a Web page. If a control is not marked as SFI, it is marked UFI, which means that it is capable of affecting a user's computer. If UFI ActiveX controls are loaded, they are always loaded in unsafe mode.

If this policy setting is enabled, choose from four options for loading controls in UserForms:

1. For a UFI or SFI signed control that supports safe and unsafe mode, load the control in unsafe mode. For an SFI signed control that only supports a safe mode configuration, load the control in safe mode. This option enforces the default configuration.
2. Users are prompted to determine how UserForm forms will load. The prompt only displays once per session within an application. When users respond to the prompt, loading continues based on whether the control is UFI or SFI:

- For a UFI signed control, if users respond "Yes" to the prompt, load the control in unsafe mode. If users respond "No", load the control using the default properties.

- For an SFI signed control that supports both safe and unsafe modes, if users respond "Yes" to the prompt, load the control in unsafe mode. If users respond "No", load the control using safe mode. If the SFI control can only support safe mode, load the control in safe mode. This option is the default configuration in the Microsoft Office 365 ProPlus release.

3. Users are prompted to determine how UserForm forms will load. The prompt only displays once per session within an application. When users respond to the prompt, loading continues based on whether the control is UFI or SFI:

- For a UFI signed control, if users respond "Yes" to the prompt, load the control in unsafe mode. If users respond "No", load the control with its default properties.
- For an SFI signed control, load in safe mode.

4. For a UFI signed control, load with the default properties of the control. For an SFI signed control, load in safe mode (considered to be the safest mode).

If this policy setting is disabled or not configured, the behavior is as if this policy setting is enabled and then select option "1".

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Load Controls in Forms3" is set to Enabled and 1 from drop down. (For a UFI or SFI signed control that supports safe and unsafe mode, load the control in unsafe mode. For an SFI signed control that only supports a safe mode configuration, load the control in safe mode. This option enforces the default configuration.)".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\\VBA\Security

If the value LoadControlsInForms is REG_DWORD=1, this is not a finding.

If the value LoadControlsInForms does not exist, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Office 2016 >> Security Settings "Load Controls in Forms3" to "Enabled:1" or set it to "Disabled."

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)

- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.16 O365-CO-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Add-on Management must be enabled for all Office 365 ProPlus programs.

```
GROUP ID: V-223296
RULE ID: SV-223296r961086
```

Rationale:

Internet Explorer add-ons are pieces of code, run in Internet Explorer, to provide additional functionality. Rogue add-ons may contain viruses or other malicious code. Disabling or not configuring this setting could allow malicious code or users to become active on user computers or the network. For example, a malicious user can monitor and then use keystrokes that user's type into Internet Explorer. Even legitimate add-ons may demand resources, compromising the performance of Internet Explorer and the operating systems for user computers.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security "Add-on Management"
```

is set to "Enabled" and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDON_MANAGEMENT

If the value for each installed Office Program is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security "Add-on Management"
```

to "Enabled" and select the check boxes for all installed Office programs.

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)

- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.17 O365-CO-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Consistent MIME handling must be enabled for all Office 365 ProPlus programs.

```
GROUP ID: V-223297
RULE ID: SV-223297r961050
```

Rationale:

Encryption is only as good as the encryption modules utilized. Unapproved cryptographic module algorithms cannot be verified and cannot be relied on to provide confidentiality or integrity, and DoD data may be compromised due to weak algorithms. The use of TLS provides confidentiality of data in transit between the application server and client. FIPS 140-2 approved TLS versions include TLS V1.0 or greater.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Consistent Mime Handling is
set to "Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling

If the value for all installed Office programs is set to is REG_DWORD=1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security "Consistent Mime Handling"
```

to "Enabled" and select the check boxes for all installed Office programs.

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.18 O365-CO-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

User name and password must be disabled in all Office programs.

```
GROUP ID: V-223298
RULE ID: SV-223298r961092
```

Rationale:

The Uniform Resource Locator (URL) standard allows user authentication to be included in URL strings in the form http://username:password@example.com. A malicious user might use this URL syntax to create a hyperlink that appears to open a legitimate website but actually opens a deceptive (spoofed) website. For example, the URL http://www.wingtiptoys.com@example.com appears to open http://www.wingtiptoys.com but actually opens http://example.com. To protect users from such attacks, Internet Explorer usually blocks any URLs using this syntax.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security "Disable user name and
password"
```

is set to "Enabled" and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security "Disable user name and
password"
```

to "Enabled" and select the check boxes for all installed Office programs.

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.19 O365-CO-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Information Bar must be enabled in all Office programs.

```
GROUP ID: V-223299
RULE ID: SV-223299r961086
```

Rationale:

This policy setting controls whether Office 365 ProPlus applications notify users when potentially unsafe features or content are detected, or whether such features or content are silently disabled without notification. The Message Bar in Office 2016 applications is used to identify security issues, such as unsigned macros or potentially unsafe add-ins. When such issues are detected, the application disables the unsafe feature or content and displays the Message Bar at the top of the active window. The Message Bar informs the users about the nature of the security issue and, in some cases, provides the users with an option to enable the potentially unsafe feature or content, which could harm the user's computer.

If you enable this policy setting, Office 365 ProPlus applications do not display information in the Message Bar about potentially unsafe content that has been detected or has automatically been blocked.

If you disable this policy setting, Office 365 ProPlus applications display information in the Message Bar about content that has automatically been blocked.

If you do not configure this policy setting, if an Office 365 ProPlus application detects a security issue, the Message Bar is displayed. However, this configuration can be modified by users in the Trust Center.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Information Bar is set to
"Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_securityband

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Information Bar to "Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.20 O365-CO-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Local Machine Zone Lockdown Security must be enabled in all Office programs.

```
GROUP ID: V-223300
RULE ID: SV-223300r961863
```

Rationale:

Internet Explorer places restrictions on each web page users can use the browser to open. Web pages on a user's local computer have the fewest security restrictions and reside in the Local Machine zone, making this security zone a prime target for malicious users and code. Disabling or not configuring this setting could allow pages in the Internet zone to navigate to pages in the Local Machine zone to then run code to elevate privileges. This could allow malicious code or users to become active on user computers or the network.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Local Machine Zone Lockdown
Security is set to "Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown

If the value for all installed Office programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Local Machine Zone Lockdown
to "Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.21 O365-CO-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The MIME Sniffing safety feature must be enabled in all Office programs.

```
GROUP ID: V-223301
RULE ID: SV-223301r961050
```

Rationale:

Encryption is only as good as the encryption modules utilized. Unapproved cryptographic module algorithms cannot be verified and cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised due to weak algorithms. The use of TLS provides confidentiality of data in transit between the application server and client. FIPS 140-2 approved TLS versions include TLS V1.0 or greater.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Mime Sniffing Safety Feature
is set to "Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing

If the value for all installed Office Programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Mime Sniffing Safety Feature
to "Enabled"
```

for all installed Office programs.

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.22 O365-CO-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Object Caching Protection must be enabled in all Office programs.

```
GROUP ID: V-223303
RULE ID: SV-223303r961050
```

Rationale:

Encryption is only as good as the encryption modules utilized. Unapproved cryptographic module algorithms cannot be verified and cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised due to weak algorithms. The use of TLS provides confidentiality of data in transit between the application server and client. FIPS 140-2 approved TLS versions include TLS V1.0 or greater.

TLS must be enabled and non-FIPS-approved SSL versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Object Caching Protection is
set to "Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_object_caching

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Object Caching Protection to
"Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.23 O365-CO-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Navigate URL must be enabled in all Office programs.

```
GROUP ID: V-223302
RULE ID: SV-223302r961092
```

Rationale:

To protect users from attacks, Internet Explorer usually does not attempt to load malformed URLs. This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a web page). If Internet Explorer attempts to load a malformed URL, a security risk could occur.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Navigate URL is set to
"Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_validate_navigate_url

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Navigate URL to "Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.24 O365-CO-000022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Protection from zone elevation must be enabled in all Office programs.

```
GROUP ID: V-223304
RULE ID: SV-223304r960921
```

Rationale:

Internet Explorer places restrictions on each web page users can use the browser to open. Web pages on a user's local computer have the fewest security restrictions and reside in the Local Machine zone, making this security zone a prime target for malicious users and code. Disabling or not configuring this setting could allow pages in the Internet zone to navigate to pages in the Local Machine zone to then run code to elevate privileges. This could allow malicious code or users to become active on user computers or the network.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Protection from Zone
Elevation is set to "Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Protection from Zone
Elevation to "Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-001695 Prevent the execution of organization-defined unacceptable mobile code.

- NIST SP 800-53::SC-18 (3)

- NIST SP 800-53 Revision 4::SC-18 (3)
- NIST SP 800-53 Revision 5::SC-18 (3)
- NIST SP 800-53A::SC-18 (3).1

1.25 O365-CO-000023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

ActiveX installation restriction must be enabled in all Office programs.

```
GROUP ID: V-223305
RULE ID: SV-223305r961779
```

Rationale:

Microsoft ActiveX controls allow unmanaged, unprotected code to run on the user computers. ActiveX controls do not run within a protected container in the browser like the other types of HTML or Microsoft Silverlight-based controls. Disabling or not configuring this setting does not block prompts for ActiveX control installations, and these prompts display to users. This could allow malicious code to become active on user computers or the network.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Restrict ActiveX Install is
set to "Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_activexinstall

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Restrict ActiveX Install to
"Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)

- NIST SP 800-53 Revision 5::SC-18 (4)

1.26 O365-CO-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

File Download Restriction must be enabled in all Office programs.

```
GROUP ID: V-223306
RULE ID: SV-223306r960921
```

Rationale:

Disabling this setting allows websites to present file download prompts via code without the user specifically initiating the download. User preferences may also allow the download to occur without prompting or interaction with the user. Even if Internet Explorer prompts the user to accept the download, some websites abuse this functionality. Malicious websites may continually prompt users to download a file or present confusing dialog boxes to trick users into downloading or running a file. If the download occurs and it contains malicious code, the code could become active on user computers or the network.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Restrict File Download is
set to "Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Restrict File Download to
"Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-001695 Prevent the execution of organization-defined unacceptable mobile code.

- NIST SP 800-53::SC-18 (3)
- NIST SP 800-53 Revision 4::SC-18 (3)
- NIST SP 800-53 Revision 5::SC-18 (3)
- NIST SP 800-53A::SC-18 (3).1

1.27 O365-CO-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Save from URL feature must be enabled in all Office programs.

```
GROUP ID: V-223307
RULE ID: SV-223307r961092
```

Rationale:

Typically, when Internet Explorer loads a web page from a Universal Naming Convention (UNC) share that contains a Mark of the Web (MOTW) comment, indicating the page was saved from a site on the Internet, Internet Explorer runs the page in the Internet security zone instead of the less restrictive Local Intranet security zone. This functionality can be controlled separately for instances of Internet Explorer spawned by Office applications (for example, if a user clicks a link in an Office document or selects a menu option that loads a web page). If Internet Explorer does not evaluate the page for a MOTW, potentially dangerous code could be allowed to run.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Saved from URL is set to
"Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Saved from URL to "Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.28 O365-CO-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Scripted Windows Security restrictions must be enabled in all Office programs.

```
GROUP ID: V-223308
RULE ID: SV-223308r960921
```

Rationale:

Malicious websites often try to confuse or trick users into giving a site permission to perform an action allowing the site to take control of the users' computers in some manner. Disabling or not configuring this setting allows unknown websites to:

- Create browser windows appearing to be from the local operating system.
- Draw active windows displaying outside of the viewable areas of the screen capturing keyboard input.
- Overlay parent windows with their own browser windows to hide important system information, choices, or prompts.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >> Scripted Window Security
Restrictions is set to "Enabled"
```

and the check box is selected for every installed Office program.

Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS

If the value for all installed programs is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Microsoft Office 2016
(Machine) >> Security Settings >> IE Security >>Scripted Window Security
Restrictions to "Enabled"
```

and select the check boxes for all installed Office programs.

Additional Information:

CCI-001695 Prevent the execution of organization-defined unacceptable mobile code.

- NIST SP 800-53::SC-18 (3)
- NIST SP 800-53 Revision 4::SC-18 (3)
- NIST SP 800-53 Revision 5::SC-18 (3)
- NIST SP 800-53A::SC-18 (3).1

1.29 O365-CO-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Flash player activation must be disabled in all Office programs.

```
GROUP ID: V-223309
RULE ID: SV-223309r961779
```

Rationale:

This policy setting controls whether the Adobe Flash control can be activated by Office documents. Note that activation blocking applies only within Office processes.

If you enable this policy setting, you can choose from three options to control whether and how Flash is blocked from activation:

1. "Block all activation" prevents the Flash control from being loaded, whether directly referenced by the document or indirectly by another embedded object.
2. "Block embedding/linking, allow other activation" prevents the Flash control from being loaded when directly referenced by the document, but does not prevent activation through another object.
3. "Allow all activation" restores Office's default behavior, allowing the Flash control to be activated.

Because this setting is not a true Group Policy setting and "tattoos" the registry, enabling the "Allow all activation" option is the only way to restore default behavior after either of the "Block" options has been applied. It is not recommended to configure this setting to "Disabled" or "Not Configured" after it has been enabled.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> MS Security Guide >>
Block Flash activation in Office documents >> Enabled >> Block all activation
is set to "Enabled"
```

Block all activation.

Use the Windows Registry Editor to navigate to the following key:

HKLM\SOFTWARE\Microsoft\Office\Common\COM Compatibility

If the value for COMMENT is REG_SZ = Block all Flash activation, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> MS Security Guide >>
Block Flash activation in Office documents >> Enabled >> Block all activation
to "Enabled"
```

(Block all activation).

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.30 O365-EX-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Trusted Locations on the network must be disabled in Excel.

```
GROUP ID: V-223310
RULE ID: SV-223310r961092
```

Rationale:

This policy setting controls whether trusted locations on the network can be used.

If you enable this policy setting, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by selecting the "Allow Trusted Locations on my network (not recommended)" check box in the Trusted Locations section of the Trust Center. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

If you disable or do not configure this policy setting, the selected application ignores any network locations listed in the Trusted Locations section of the Trust Center. Disabling this policy setting does not delete any network locations from the Trusted Locations list. Instead, it forces the selected application to treat the locations as non-trusted and prevents users from adding new network locations to the list.

If you also deploy Trusted Locations via Group Policy, you should verify whether any of them are remote locations. If any of them are remote locations and you do not allow remote locations via this policy setting, those policy keys that point to remote locations will be ignored on client computers.

Disabling this policy setting will cause disruption for users who add network locations to the Trusted Locations list. However, it is not recommended to enable this policy setting (as the "Allow Trusted Locations on my network (not recommended)" check box itself states), so in practice it should be possible to disable this policy setting in most situations without causing significant usability issues for most users.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Trusted Locations "Allow Trusted Locations on the network" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\trusted locations

If the value AllowNetworkLocations is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Trusted Locations "Allow Trusted Locations on the network" to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.31 O365-EX-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VBA Macros not digitally signed must be blocked in Excel.

```
GROUP ID: V-223311
RULE ID: SV-223311r960963
```

Rationale:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If you enable this policy setting, you can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office. This option also allows users to potentially enable unsigned/untrusted macros. If a site requires the use of macros, they must be signed /approved and added to appropriate locations listed in the Trust Center Settings.
- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.
- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.
- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> "Macro Notification Settings" is set to "Enabled" and "Disable VBA macros except digitally signed macros" from the Options is selected.

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\excel\security

If the value vbawarnings is REG_DWORD = 3, this is not a finding. A value of REG_DWORD = 4 is also acceptable. If the registry key does not exist or is not configured properly, this is a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> "Macro Notification Settings" is set to "Enabled" and select "Disable VBA macros except digitally signed macros" from the Options.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.32 O365-EX-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Dynamic Data Exchange (DDE) server launch in Excel must be blocked.

```
GROUP ID: V-223312
RULE ID: SV-223312r961086
```

Rationale:

This policy setting allows you to control whether Dynamic Data Exchange (DDE) server launch is allowed.

By default, DDE server launch is turned off, but users can turn on DDE server launch by going to File >> Options >> Trust Center >> Trust Center Settings >> External Content.

For security reasons, turning on DDE server launch is not recommended.

Note: For DDE server launch to work, Dynamic Data Exchange (DDE) server lookup must be turned on. Be sure that the “Don't allow Dynamic Data Exchange (DDE) server lookup” policy setting is not enabled, because enabling that policy setting turns off DDE server lookup.

If you enable this policy setting, DDE server launch is not allowed, and users cannot turn on DDE server launch in the Trust Center.

If you disable this policy setting, DDE server launch is allowed, and users cannot turn off DDE server launch in the Trust Center. For security reasons, this is not recommended.

If you do not configure this policy setting, DDE server launch is turned off, but users can turn on DDE server launch in the Trust Center.

Note: This policy setting only applies to subscription versions of Office, such as Office 365 ProPlus.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> External Content >> Don't allow Dynamic Data Exchange (DDE) server launch in Excel is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\external content

If the value for "disableddeserverlaunch" is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> External Content >> Don't allow Dynamic Data Exchange (DDE) server launch in Excel to "Enabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.33 O365-EX-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Dynamic Data Exchange (DDE) server lookup in Excel must be blocked.

```
GROUP ID: V-223313
RULE ID: SV-223313r961086
```

Rationale:

This policy setting allows you to control whether Dynamic Data Exchange (DDE) server lookup is allowed.

By default, DDE server lookup is turned on, but users can turn off DDE server lookup by going to File >> Options >> Trust Center >> Trust Center Settings >> External Content.

If you enable this policy setting, DDE server lookup is not allowed, and users cannot turn on DDE server lookup in the Trust Center.

Note: If you are using Dynamic Data Exchange (DDE) server launch, which is not recommended, do not enable this policy setting, because DDE server launch requires DDE server lookup to be on.

If you disable or do not configure this policy setting, DDE server lookup is turned on, but users can turn off DDE server lookup in the Trust Center.

Note: This policy setting only applies to subscription versions of Office, such as Office 365 ProPlus.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> External Content >> Don't allow Dynamic Data Exchange (DDE) server lookup in Excel is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\external content

If the value for "disableddeserverlookup" is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> External Content >> Don't allow Dynamic Data Exchange (DDE) server lookup in Excel to "Enabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.34 O365-EX-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of dBase III / IV format files must be blocked.

```
GROUP ID: V-223314
RULE ID: SV-223314r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "dBase III / IV files" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value DBaseFiles is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "dBase III / IV files" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.35 O365-EX-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 2 macrosheets and add-in files must be blocked.

```
GROUP ID: V-223316
RULE ID: SV-223316r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 2 macrosheets and add-in files" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value XL2Macros is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 2 macrosheets and add-in files" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.36 O365-EX-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Dif and Sylk format files must be blocked.

```
GROUP ID: V-223315
RULE ID: SV-223315r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Dif and Sylk files" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value DifandSylkFiles is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Dif and Sylk files" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.37 O365-EX-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 2 worksheets must be blocked.

```
GROUP ID: V-223317
RULE ID: SV-223317r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 2 worksheets" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value XL2Worksheets is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 2 worksheets" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.38 O365-EX-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 3 macrosheets and add-in files must be blocked.

```
GROUP ID: V-223318
RULE ID: SV-223318r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 3 macrosheets and add-in files" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value XL3Macros is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 3 macrosheets and add-in files" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.39 O365-EX-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 3 worksheets must be blocked.

```
GROUP ID: V-223319
RULE ID: SV-223319r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 3 worksheets" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value XL3Worksheets is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 3 worksheets" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.40 O365-EX-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 4 macrosheets and add-in files must be blocked.

```
GROUP ID: V-223320
RULE ID: SV-223320r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 4 macrosheets and add-in files" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value XL4Macros is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 4 macrosheets and add-in files" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.41 O365-EX-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 4 workbooks must be blocked.

```
GROUP ID: V-223321
RULE ID: SV-223321r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 4 workbooks" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value XL4Workbooks is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 4 workbooks" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.42 O365-EX-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 4 worksheets must be blocked.

```
GROUP ID: V-223322
RULE ID: SV-223322r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 4 worksheets" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value XL4Worksheets is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 4 worksheets" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.43 O365-EX-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 95 workbooks must be blocked.

```
GROUP ID: V-223323
RULE ID: SV-223323r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings >> Excel 95 workbooks is set to "Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\fileblock

If the value for xl95workbooks is REG_DWORD = 2, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings >> Excel 95 workbooks to "Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.44 O365-EX-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Excel 95-97 workbooks and templates must be blocked.

```
GROUP ID: V-223324
RULE ID: SV-223324r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 95-97 workbooks and templates" is set to "Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\office\16.0\excel\security\fileblock

If the value XL9597WorkbooksandTemplates is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings "Excel 95-97 workbooks and templates" to "Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.45 O365-EX-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The default file block behavior must be set to not open blocked files in Excel.

```
GROUP ID: V-223325
RULE ID: SV-223325r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings >> Set default file block behavior is set to "Blocked files are not opened".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\fileblock

If the value OpenInProtectedView is REG_DWORD = 0, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings >> Set default file block behavior to "Enabled:Blocked files are not opened".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.46 O365-EX-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/save of Web pages and Excel 2003 XML spreadsheets must be blocked.

```
GROUP ID: V-223326
RULE ID: SV-223326r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Excel files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings >> Web pages and Excel 2003 XML spreadsheets is set to "Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\fileblock

If the value for htmlandxmlssfiles is REG_DWORD = 2, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> File Block Settings >> Web pages and Excel 2003 XML spreadsheets to "Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.47 O365-EX-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Extraction options must be blocked when opening corrupt Excel workbooks.

```
GROUP ID: V-223327
RULE ID: SV-223327r961086
```

Rationale:

This policy setting controls whether Excel presents users with a list of data extraction options before beginning an Open and Repair operation when users choose to open a corrupt workbook in repair or extract mode.

If you enable this policy setting, Excel opens the file using the Safe Load process and does not prompt users to choose between repairing or extracting data.

If you disable or do not configure this policy setting, Excel prompts the user to select either to repair or to extract data, and to select either to convert to values or to recover formulas.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Data Recovery >> Do not show data extraction options when opening corrupt workbooks is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\options

If the value for extractdatadisableui is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Data Recovery >> Do not show data extraction options when opening corrupt workbooks to "Enabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)

- NIST SP 800-53 Revision 5::SC-18 (1)

1.48 O365-EX-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Updating of links in Excel must be prompted and not automatic.

```
GROUP ID: V-223328
RULE ID: SV-223328r961092
```

Rationale:

This policy setting controls whether Excel prompts users to update automatic links, or whether the updates occur in the background with no prompt.

If you enable or do not configure this policy setting, Excel will prompt users to update automatic links. In addition, the "Ask to update automatic links" user interface option under File tab >> Advanced >> General is selected.

If you disable this policy setting, Excel updates automatic links without prompting or informing users, which could compromise the integrity of some of the information in the workbook.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Advanced >> Ask to update automatic links is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\options\binaryoptions

If the value for fupdateext_78_1 is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Advanced >> Ask to update automatic links to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)

- NIST SP 800-53 Revision 5::SC-18 (4)

1.49 O365-EX-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Loading of pictures from Web pages not created in Excel must be disabled.

```
GROUP ID: V-223329
RULE ID: SV-223329r961779
```

Rationale:

This policy setting controls whether Excel loads graphics when opening Web pages that were not created in Excel. It configures the "Load pictures from Web pages not created in Excel" option under the File tab >> Options >> Advanced >> General >> Web Options... >> General tab.

If you enable or do not configure this policy setting, Excel loads any graphics that are included in the pages, regardless of whether they were originally created in Excel.

If you disable this policy setting, Excel will not load any pictures from Web pages that were not created in Excel.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Advanced >> Web Options... >> General.

Load pictures from Web pages not created in Excel is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\internet

If the value for donotloadpictures is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Advanced >> Web Options... >> General >> Load pictures from Web pages not created in Excel to "Disabled".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.50 O365-EX-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

AutoRepublish in Excel must be disabled.

```
GROUP ID: V-223330
RULE ID: SV-223330r961863
```

Rationale:

This policy setting allows administrators to disable the AutoRepublish feature in Excel. If users choose to publish Excel data to a static Web page and enable the AutoRepublish feature, Excel saves a copy of the data to the Web page every time the user saves the workbook. By default, a message dialog displays every time the user saves a published workbook when AutoRepublish is enabled. From this dialog, the user can disable AutoRepublish temporarily or permanently, or select "Do not show this message again" to prevent the dialog from appearing after every save. If the user selects "Do not show this message again", Excel will continue to automatically republish the data after every save without informing the user.

If you enable this policy setting, the AutoRepublish feature is turned off and Excel users will need to publish data to the Web manually.

If you disable or do not configure this policy setting, users can enable the AutoRepublish feature to automatically republish workbooks saved as type Web Page.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Save >> Disable AutoRepublish is to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\options

If the value for disableautorepublish is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Save >> Disable AutoRepublish to "Enabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b

- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.51 O365-EX-000022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

AutoRepublish warning alert in Excel must be enabled.

```
GROUP ID: V-223331
RULE ID: SV-223331r961863
```

Rationale:

This policy setting allows administrators to disable the AutoRepublish feature in Excel. If users choose to publish Excel data to a static Web page and enable the AutoRepublish feature, Excel saves a copy of the data to the Web page every time the user saves the workbook. By default, a message dialog displays every time the user saves a published workbook when AutoRepublish is enabled. From this dialog, the user can disable AutoRepublish temporarily or permanently, or select "Do not show this message again" to prevent the dialog from appearing after every save. If the user selects "Do not show this message again", Excel will continue to automatically republish the data after every save without informing the user.

If you enable this policy setting, the AutoRepublish feature is turned off and Excel users will need to publish data to the Web manually.

If you disable or do not configure this policy setting, users can enable the AutoRepublish feature to automatically republish workbooks saved as type Web Page.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Save >> Do not show AutoRepublish warning alert is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\options

If value for disableautorepublishwarning is REG_DWORD = 0, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Save >> Do not show AutoRepublish warning alert to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.52 O365-EX-000023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

File extensions must be enabled to match file types in Excel.

```
GROUP ID: V-223332
RULE ID: SV-223332r961863
```

Rationale:

This policy setting controls how Excel loads file types that do not match their extension. Excel can load files with extensions that do not match the files' type. For example, if a comma-separated values (CSV) file named example.csv is renamed example.xls (or any other file extension supported by Excel 2003 and earlier only), Excel can properly load it as a CSV file.

If you enable this policy setting, you can choose from three options for working with files that have non-matching extensions:

- Allow different - Excel opens the files properly without warning users that the files have non-matching extensions. If users subsequently edit and save the files, Excel preserves both the true, underlying file format and the incorrect file extension.
- Allow different, but warn - Excel opens the files properly, but warns users about the file type mismatch. This option is the default configuration in Excel.
- Always match file type - Excel does not open any files that have non-matching extensions.

If this policy setting is disabled or not configured or if users attempt to open files with the wrong extension, Excel opens the file and displays a warning that the file type is not what Excel expected.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Force file extension to match file type is set to "Always match file type".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security

If value for extensionhardening is REG_DWORD = 2, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Force file extension to match file type to "Enabled" and select the option "Always match file type".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.53 O365-EX-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Scan of encrypted macros in Excel Open XML workbooks must be enabled.

```
GROUP ID: V-223333
RULE ID: SV-223333r961092
```

Rationale:

This policy setting controls whether encrypted macros in Open XML workbooks be are required to be scanned with anti-virus software before being opened.

If you enable this policy setting, you may choose one of these options:

- Scan encrypted macros: encrypted macros are disabled unless anti-virus software is installed. Encrypted macros are scanned by your anti-virus software when you attempt to open an encrypted workbook that contains macros.
- Scan if anti-virus software available: if anti-virus software is installed, scan the encrypted macros first before allowing them to load. If anti-virus software is not available, allow encrypted macros to load.
- Load macros without scanning: do not check for anti-virus software and allow macros to be loaded in an encrypted file.

If you disable or do not configure this policy setting, the behavior will be similar to the "Scan encrypted macros" option.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Scan encrypted macros in Excel Open XML workbooks is set to "Scan encrypted macros (default)".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security

If the value excelbypassencryptedmacroscan does not exist, this is not a finding.

If the value for excelbypassencryptedmacroscan is REG_DWORD = 0, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Scan encrypted macros in Excel Open XML workbooks to "Scan encrypted macros (default)".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.54 O365-EX-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

File validation in Excel must be enabled.

```
GROUP ID: V-223334
RULE ID: SV-223334r960921
```

Rationale:

This policy setting allows you turn off the file validation feature.

If you enable this policy setting, file validation will be turned off.

If you disable or do not configure this policy setting, file validation will be turned on. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Turn off file validation is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\filevalidation

If the value for enableonload is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Turn off file validation to "Disabled".

Additional Information:

CCI-001695 Prevent the execution of organization-defined unacceptable mobile code.

- NIST SP 800-53::SC-18 (3)
- NIST SP 800-53 Revision 4::SC-18 (3)
- NIST SP 800-53 Revision 5::SC-18 (3)
- NIST SP 800-53A::SC-18 (3).1

1.55 O365-EX-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

WEBSERVICE Function Notification in Excel must be configured to disable all, with notifications.

```
GROUP ID: V-223335
RULE ID: SV-223335r961086
```

Rationale:

This policy setting controls how Excel will warn users when WEBSERVICE functions are present.

If you enable this policy setting, you can choose from three options for determining how the specified applications will warn the user about WEBSERVICE functions:

- Disable all with notification: The application displays the Trust Bar for all WEBSERVICE functions. This option enforces the default configuration in Office.
- Disable all without notification: The application disables all WEBSERVICE functions and does not notify users.
- Enable all WEBSERVICE functions (not recommended): The application enables all WEBSERVICE functions and does not notify users. This option can significantly reduce security by allowing information disclosure to third-party web services.

If you disable this policy setting, the “Disable all with notification” will be the default setting.

If you do not configure this policy setting, when users open workbooks that contain WEBSERVICE functions, Excel will open the files with the WEBSERVICE functions disabled and display the Trust Bar with a warning that WEBSERVICE functions are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content," then the document is added as a trusted document.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> WEBSERVICE Function Notification Settings is set to "Enabled" and "Disable all with notification".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security

If the value webservicefunctionwarnings does not exist, this is not a finding.

If the value for webservicefunctionwarnings is REG_DWORD = 1, this is not a finding.

If the value for webservicefunctionwarnings is REG_DWORD = 2, this is a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> WEBSERVICE Function Notification Settings to "Enabled" and "Disable all with notification".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.56 O365-EX-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Macros must be blocked from running in Excel files from the Internet.

```
GROUP ID: V-223336
RULE ID: SV-223336r961092
```

Rationale:

This policy setting allows you to block macros from running in Office files that come from the Internet.

If you enable this policy setting, macros are blocked from running, even if “Enable all macros” is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to “Enable Content”, users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

If you disable or do not configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Block macros from running in Office files from the Internet is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security

If the value blockcontentexecutionfrominternet is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Block macros from running in Office files from the Internet to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.57 O365-EX-000028 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Trust Bar notification must be enabled for unsigned application add-ins in Excel and blocked.

```
GROUP ID: V-223337
RULE ID: SV-223337r1016168
```

Rationale:

This policy setting controls whether the specified Office 2016 applications notify users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if the "Require that application add-ins are signed by Trusted Publisher" policy setting is enabled, which prevents users from changing this policy setting.

If this policy setting is enabled, applications automatically disable unsigned add-ins without informing users.

If this policy setting is disabled, if an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If this policy setting is not configured, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Disable Trust Bar Notification for unsigned application add-ins and block them is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security

If the value for notbpromptunsignedaddin is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Disable Trust Bar Notification for unsigned application add-ins and block them to "Enabled".

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.58 O365-EX-000029 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Untrusted Microsoft Query files must be blocked from opening in Excel.

```
GROUP ID: V-223338
RULE ID: SV-223338r961086
```

Rationale:

This policy setting controls whether Microsoft Query files (.iqy, oqy, .dqy, and .rqy) in an untrusted location are prevented from opening.

If you enable this policy setting, Microsoft Query files in an untrusted location are prevented from opening. Users will not be able to change this setting under File >> Options >> Trust Center >> Trust Center Settings >> External Content.

If you disable or do not configure this policy setting, Microsoft Query files in an untrusted location are not prevented from opening, unless users have changed this setting in the Trust Center.

Note: This policy setting only applies to subscription versions of Office, such as Office 365 ProPlus.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> External Content >> Always prevent untrusted Microsoft Query files from opening is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\excel\security\external content.

Value for enableblockunsecurequeryfiles should be REG_DWORD = 1

If the value for enableblockunsecurequeryfiles is Reg_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> External Content >> Always prevent untrusted Microsoft Query files from opening to "Enabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.59 O365-EX-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Untrusted database files must be opened in Excel in Protected View mode.

```
GROUP ID: V-223339
RULE ID: SV-223339r961086
```

Rationale:

This policy setting controls whether database files (.dbf) opened from an untrusted location are always opened in Protected View.

If you enable this policy setting, database files opened from an untrusted location are always opened in Protected View. Users will not be able to change this setting under File >> Options >> Trust Center >> Trust Center Settings >> Protected View.

If you disable or do not configure this policy setting, database files opened from an untrusted location are not opened in Protected View, unless users have changed this setting in the Trust Center.

Note: This policy setting only applies to subscription versions of Office, such as Office 365 ProPlus.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Always open untrusted database files in Protected View is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\protectedview

If the value for enabledatabasefileprotectedview is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Always open untrusted database files in Protected View to "Enabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.60 O365-EX-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files from Internet zone must be opened in Excel in Protected View mode.

```
GROUP ID: V-223340
RULE ID: SV-223340r961086
```

Rationale:

This policy setting allows you to determine if files downloaded from the Internet zone open in Protected View.

If you enable this policy setting, files downloaded from the Internet zone do not open in Protected View.

If you disable or do not configure this policy setting, files downloaded from the Internet zone open in Protected View.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Do not open files from the Internet zone in Protected View is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\protectedview

If the value DisableInternetFilesInPV is REG_DWORD = 0, this is not a finding.

If the value does not exist, this is not a finding.

If the value is REG_DWORD = 1, this is a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Do not open files from the Internet zone in Protected View to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)

- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.61 O365-EX-000032 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files from unsafe locations must be opened in Excel in Protected View mode.

```
GROUP ID: V-223341
RULE ID: SV-223341r961092
```

Rationale:

This policy setting lets you determine if files located in unsafe locations will open in Protected View. If you have not specified unsafe locations, only the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations.

If you enable this policy setting, files located in unsafe locations do not open in Protected View.

If you disable or do not configure this policy setting, files located in unsafe locations open in Protected View.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Do not open files in unsafe locations in Protected View is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\protectedview

If the value DisableUnsafeLocationsInPV is REG_DWORD = 0, this is not a finding.

If the value does not exist, this is not a finding.

If the value is REG_DWORD = 1, this is a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Do not open files in unsafe locations in Protected View to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)

- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.62 O365-EX-000033 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files failing file validation must be opened in Excel in Protected view mode and disallow edits.

```
GROUP ID: V-223342
RULE ID: SV-223342r961092
```

Rationale:

This policy setting controls how Office handles documents when they fail file validation.

If you enable this policy setting, you can configure the following options for files that fail file validation:

- Block files completely. Users cannot open the files.
- Open files in Protected View and disallow edit. Users cannot edit the files. This is also how Office handles the files if you disable this policy setting.
- Open files in Protected View and allow edit. Users can edit the files. This is also how Office handles the files if you do not configure this policy setting.

If you disable this policy setting, Office follows the "Open files in Protected View and disallow edit" behavior.

If you do not configure this policy setting, Office follows the "Open files in Protected View and allow edit" behavior.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Set document behavior if file validation fails is set to "Enabled: Open in Protected View". Verify the check box for "Allow edit" is not selected.

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\Excel\security\filevalidation

If the value openinprotectedview does not exist, this is not a finding.

If both the value for openinprotectedview is REG_DWORD = 1 and the value for DisableEditFromPV is set to REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Set document behavior if file validation fails to "Enabled: Open in Protected View".

Uncheck the "Allow edit" check box.

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.63 O365-EX-000034 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

File attachments from Outlook must be opened in Excel in Protected mode.

```
GROUP ID: V-223343
RULE ID: SV-223343r961092
```

Rationale:

This policy setting allows you to determine if Excel files in Outlook attachments open in Protected View.

If you enable this policy setting, Outlook attachments do not open in Protected View.

If you disable or do not configure this policy setting, Outlook attachments open in Protected View.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Turn off Protected View for attachments opened from Outlook is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\excel\security\protectedview

If the value DisableAttachmentsInPV is REG_DWORD = 0, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Excel 2016 >> Excel Options >> Security >> Trust Center >> Protected View >> Turn off Protected View for attachments opened from Outlook to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.64 O365-LY-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SIP security mode in Lync must be enabled.

```
GROUP ID: V-223344
RULE ID: SV-223344r1043178
```

Rationale:

When Lync connects to the server, it supports various authentication mechanisms. This policy allows the user to specify whether Digest and Basic authentication are supported. Disabled (default): NTLM/Kerberos/TLS-DSK/Digest/Basic Enabled: Authentication mechanisms: NTLM/Kerberos/TLS-DSK Gal Download: Requires HTTPS if user is not logged in as an internal user.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Skype for Business 2016
>> Microsoft Lync Feature Policies "Configure SIP security mode"
```

is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\office\16.0\lync

If the value enablesiphighsecuritymode is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Skype for Business 2016
>> Microsoft Lync Feature Policies "Configure SIP security mode"
```

to "Enabled".

Additional Information:

CCI-001184 Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

1.65 O365-LY-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The HTTP fallback for SIP connection in Lync must be disabled.

```
GROUP ID: V-223345
RULE ID: SV-223345r1043178
```

Rationale:

Prevents from HTTP being used for SIP connection in case TLS or TCP fail.

Audit:

Verify the policy value for

```
Computer Configuration >> Administrative Templates >> Skype for Business 2016
>> Microsoft Lync Feature Policies "Disable HTTP fallback for SIP connection"
```

is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\office\16.0\lync

If the value disablehttpconnect is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for

```
Computer Configuration >> Administrative Templates >> Skype for Business 2016
>> Microsoft Lync Feature Policies "Disable HTTP fallback for SIP connection"
```

to "Enabled".

Additional Information:

CCI-001184 Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

1.66 O365-OU-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange client authentication with Exchange servers must be enabled to use Kerberos Password Authentication.

```
GROUP ID: V-223346
RULE ID: SV-223346r961878
```

Rationale:

This policy setting controls which authentication method Outlook uses to authenticate with Microsoft Exchange Server. Note: Exchange Server supports the Kerberos authentication protocol and NTLM for authentication. The Kerberos protocol is the more secure authentication method and is supported on Windows 2000 Server and later versions. NTLM authentication is supported in pre-Windows 2000 environments.

If you enable this policy setting, you can choose from three different options for controlling how Outlook authenticates with Microsoft Exchange Server:

- Kerberos/NTLM password authentication. Outlook attempts to authenticate using the Kerberos authentication protocol. If this attempt fails, Outlook attempts to authenticate using NTLM. This option is the default configuration.
- Kerberos password authentication. Outlook attempts to authenticate using the Kerberos protocol only.
- NTLM password authentication. Outlook attempts to authenticate using NTLM only.

If you disable or do not configure this policy setting, Outlook will attempt to authenticate using the Kerberos authentication protocol. If it cannot (because no Windows 2000 or later domain controllers are available), it will authenticate using NTLM.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Account Settings >> Exchange >> Authentication with Exchange Server is set to Kerberos Password Authentication.

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value authenticationservice is set to REG_DWORD = 16 (decimal) or 10 (hex), this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Account Settings >> Exchange >> Authentication with Exchange Server to Kerberos Password Authentication.

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

1.67 O365-OU-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Outlook must use remote procedure call (RPC) encryption to communicate with Microsoft Exchange servers.

```
GROUP ID: V-223347
RULE ID: SV-223347r961878
```

Rationale:

This policy setting controls whether Outlook uses remote procedure call (RPC) encryption to communicate with Microsoft Exchange servers.

If you enable this policy setting, Outlook uses RPC encryption when communicating with an Exchange server. Note: RPC encryption only encrypts the data from the Outlook client computer to the Exchange server. It does not encrypt the messages themselves as they traverse the Internet.

If you disable or do not configure this policy setting, RPC encryption is still used by default. This setting allows you to override the corresponding per-profile setting.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Account Settings >> Exchange >> Enable RPC encryption is set to "Enabled".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\rpc

If the value for enablerpcencryption is set to REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Account Settings >> Exchange >> Enable RPC encryption to "Enabled".

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)

- NIST SP 800-53 Revision 5::IA-3 (1)

1.68 O365-OU-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Scripts associated with public folders must be prevented from execution in Outlook.

```
GROUP ID: V-223348
RULE ID: SV-223348r961092
```

Rationale:

This policy setting controls whether Outlook executes scripts that are associated with custom forms or folder home pages for public folders.

Audit:

Verify the policy for Microsoft Outlook 2016 >> Outlook Options >> Other >> Advanced >> Do not allow Outlook object model scripts to run for public folders is set to "Enabled".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for publicfolderscript is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Outlook Options >> Other >> Advanced >> Do not allow Outlook object model scripts to run for public folders to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.69 O365-OU-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Scripts associated with shared folders must be prevented from execution in Outlook.

```
GROUP ID: V-223349
RULE ID: SV-223349r961092
```

Rationale:

This policy setting controls whether Outlook executes scripts associated with custom forms or folder home pages for shared folders.

Audit:

Verify the policy for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Outlook Options >> Other >> Advanced >> Do not allow Outlook object model scripts to run for shared folders is set to "Enabled".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for sharedfolderscript is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Outlook Options >> Other >> Advanced >> Do not allow Outlook object model scripts to run for shared folders to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.70 O365-OU-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files dragged from an Outlook e-mail to the file system must be created in ANSI format.

```
GROUP ID: V-223350
RULE ID: SV-223350r961863
```

Rationale:

This policy setting controls whether e-mail messages dragged from Outlook to the file system are saved in Unicode or ANSI format.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Outlook Options >> Other >> Advanced >> Use Unicode format when dragging e-mail message to file system is set to "Disabled".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\options\general

If the value for msgformat is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Outlook Options >> Other >> Advanced >> Use Unicode format when dragging e-mail message to file system to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.71 O365-OU-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The junk email protection level must be set to No Automatic Filtering.

```
GROUP ID: V-223351
RULE ID: SV-223351r961863
```

Rationale:

This policy setting controls the Junk E-mail protection level. The Junk E-mail Filter in Outlook helps to prevent junk email messages, also known as spam, from cluttering a user's Inbox. The filter evaluates each incoming message based on several factors, including the time when the message was sent and the content of the message. The filter does not single out any particular sender or message type, but instead analyzes each message based on its content and structure to determine if it is likely spam.

A Junk E-mail filtering option of "No Automatic Filtering" will evaluate emails against domain names and email addresses in the blocked sender list and send them to the Junk E-mail folder.

A Junk E-mail filtering option of "High" is not recommended when behind enterprise-level capabilities such as Enterprise Email Security Gateway (EEMSG), Cloud-Based Internet Isolation (CBII), and O365 Exchange Online Protection (EOP).

Audit:

Note: If the Outlook client application is not used to access Office 365 email (i.e., email is only accessed via Outlook Web Access [OWA]), this check is not applicable.

Verify Outlook Junk E-mail protection is set to "No Automatic Filtering".

In Outlook, click Home tab >> Delete group >> Junk >> Junk E-mail Options.

Verify Junk E-mail protection is set to "No Automatic Filtering".

If the system being inspected is not behind EEMSG, CBII, or O365 EOP, the Junk E-mail protection level must be set to "High".

If Junk E-mail protection is not set to "No Automatic Filtering", this is a finding.

If the system is not behind enterprise-level capabilities such as EEMSG, CBII, or O365 EOP and the Junk E-mail protection is not set to "High", this is a finding.

Remediation:

In Outlook, click Home tab >> Delete group >> Junk >> Junk E-mail Options.

Set the Junk E-mail protection level to "No Automatic Filtering".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.72 O365-OU-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Active X One-Off forms must only be enabled to load with Outlook Controls.

```
GROUP ID: V-223352
RULE ID: SV-223352r961092
```

Rationale:

By default, third-party ActiveX controls are not allowed to run in one-off forms in Outlook. You can change this behavior so that Safe Controls (Microsoft Forms 2.0 controls and the Outlook Recipient and Body controls) are allowed in one-off forms, or so that all ActiveX controls are allowed to run.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Allow Active X One Off Forms is set to "Enabled" "Load only Outlook Controls".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for allowactivexoneoffforms is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Allow Active X One Off Forms to "Enabled" "Load only Outlook Controls".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.73 O365-OU-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Outlook must be configured to prevent users overriding attachment security settings.

```
GROUP ID: V-223353
RULE ID: SV-223353r961353
```

Rationale:

This policy setting prevents users from overriding the set of attachments blocked by Outlook.

If you enable this policy setting users will be prevented from overriding the set of attachments blocked by Outlook. Outlook also checks the "Level1Remove" registry key when this setting is specified.

If you disable or do not configure this policy setting, users will be allowed to override the set of attachments blocked by Outlook.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Prevent users from customizing attachment security settings is set to "Enabled".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook

If the value for disallowattachmentcustomization is set to REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Prevent users from customizing attachment security settings to "Enabled".

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

1.74 O365-OU-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Internet must not be included in Safe Zone for picture download in Outlook.

```
GROUP ID: V-223354
RULE ID: SV-223354r961863
```

Rationale:

This policy setting controls whether pictures and external content in HTML e-mail messages from untrusted senders on the Internet are downloaded without Outlook users explicitly choosing to do so.

If you enable this policy setting, Outlook will automatically download external content in all e-mail messages sent over the Internet and users will not be able to change the setting.

If you disable or do not configure this policy setting, Outlook does not consider the Internet a safe zone, which means that Outlook will not automatically download content from external servers unless the sender is included in the Safe Senders list. Recipients can choose to download external content from untrusted senders on a message-by-message basis.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Automatic Picture Download Settings >> Include Internet in Safe Zones for Automatic Picture Download is set to "Disabled".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\options\mail

If the value for Internet is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Automatic Picture Download Settings >> Include Internet in Safe Zones for Automatic Picture Download to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b

- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.75 O365-OU-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Publish to Global Address List (GAL) button must be disabled in Outlook.

```
GROUP ID: V-223355
RULE ID: SV-223355r961863
```

Rationale:

This policy setting controls whether Outlook users can publish e-mail certificates to the Global Address List (GAL).

If you enable this policy setting, the "Publish to GAL" button does not display in the "E-mail Security" section of the Trust Center.

If you disable or do not configure this policy setting, Outlook users can publish their e-mail certificates to the GAL through the "E-mail Security" section of the Trust Center.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Cryptography >> Do not display 'Publish to GAL' button is set to "Enabled".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for publishtogaldisabled is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Cryptography >> Do not display 'Publish to GAL' button to "Enabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.76 O365-OU-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The minimum encryption key length in Outlook must be at least 168.

```
GROUP ID: V-223356
RULE ID: SV-223356r961905
```

Rationale:

This policy setting allows you to set the minimum key length for an encrypted e-mail message.

If you enable this policy setting, you may set the minimum key length for an encrypted e-mail message. Outlook will display a warning dialog if the user tries to send a message using an encryption key that is below the minimum encryption key value set. The user can still choose to ignore the warning and send using the encryption key originally chosen.

If you disable or do not configure this policy setting, a dialog warning will be shown to the user if the user attempts to send a message using encryption. The user can still choose to ignore the warning and send using the encryption key originally chosen.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Cryptography >> Minimum encryption settings is set to "Enabled" and a Minimum key size (in bits) of "168" or above.

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for minenckey is set to 168 or above, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Cryptography >> Minimum encryption settings to "Enabled"and a Minimum key size (in bits) of "168" or above.

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13

- NIST SP 800-53 Revision 5::SC-13 b

1.77 O365-OU-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The warning about invalid digital signatures must be enabled to warn Outlook users.

```
GROUP ID: V-223357
RULE ID: SV-223357r961086
```

Rationale:

This policy setting controls how Outlook warns users about messages with invalid digital signatures.

If you enable this policy setting, you can choose from three options for controlling how Outlook users are warned about invalid signatures:

- Let user decide if they want to be warned. This option enforces the default configuration.
- Always warn about invalid signatures.
- Never warn about invalid signatures.

If you disable or do not configure this policy setting, if users open e-mail messages that include invalid digital signatures, Outlook displays a warning dialog. Users can decide whether they want to be warned about invalid signatures in the future.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Cryptography >> Signature Warning is set to "Enabled" "Always warn about invalid signatures".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for warnaboutinvalid is set to REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Cryptography >> Signature Warning to "Enabled" "Always warn about invalid signatures".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.78 O365-OU-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Outlook must be configured to allow retrieving of Certificate Revocation Lists (CRLs) always when online.

```
GROUP ID: V-223358
RULE ID: SV-223358r961893
```

Rationale:

This policy setting controls how Outlook retrieves Certificate Revocation Lists to verify the validity of certificates. Certificate revocation lists (CRLs) are lists of digital certificates that have been revoked by their controlling certificate authorities (CAs), typically because the certificates were issued improperly or their associated private keys were compromised.

If you enable this policy setting, you can choose from three options to govern how Outlook uses CRLs:

- Use system Default. Outlook relies on the CRL download schedule that is configured for the operating system.
- When online always retrieve the CRL. This option is the default configuration in Outlook.
- Never retrieve the CRL. Outlook will not attempt to download the CRL for a certificate, even if it is online. This option can reduce security.

If you disable or do not configure this policy setting, when Outlook handles a certificate that includes a URL from which a CRL can be downloaded, Outlook will retrieve the CRL from the provided URL if Outlook is online.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Cryptography >> Signature Status dialog box >> Retrieving CRLs (Certificate Revocation Lists) is set to "Enabled" "When online always retrieve the CRL".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for usecrlchasing is set to REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Cryptography >> Signature Status dialog box >> Retrieving CRLs (Certificate Revocation Lists) to "Enabled" "When online always retrieve the CRL".

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

1.79 O365-OU-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Outlook Security Mode must be enabled to always use the Outlook Security Group Policy.

```
GROUP ID: V-223359
RULE ID: SV-223359r961863
```

Rationale:

This policy setting controls which set of security settings are enforced in Outlook. If you enable this policy setting, you can choose from four options for enforcing Outlook security settings:

- Outlook Default Security - This option is the default configuration in Outlook. Users can configure security themselves, and Outlook ignores any security-related settings configured in Group Policy.
- Use Security Form from "Outlook Security Settings" Public Folder - Outlook uses the settings from the security form published in the designated public folder.
- Use Security Form from "Outlook 10 Security Settings" Public Folder - Outlook uses the settings from the security form published in the designated public folder.
- Use Outlook Security Group Policy - Outlook uses security settings from Group Policy. Important: You must enable this policy setting if you want to apply the other Outlook security policy settings mentioned in this guide. If you disable or do not configure this policy setting, Outlook users can configure security for themselves, and Outlook ignores any security-related settings that are configured in Group Policy.

Note: In previous versions of Outlook, when security settings were published in a form in Exchange Server public folders, users who needed these settings required the HKEY_CURRENT_USER >> Software >> Policies >> Microsoft >> Security >> CheckAdminSettings registry key to be set on their computers for the settings to apply. In Outlook, the CheckAdminSettings registry key is no longer used to determine users' security settings. Instead, the Outlook Security Mode setting can be used to determine whether Outlook security should be controlled directly by Group Policy, by the security form from the Outlook Security Settings Public Folder, or by the settings on users' own computers.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Outlook Security Mode is set to "Enabled (Use Outlook Security Group Policy)".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for adminsecuritymode is set to REG_DWORD = 3, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Outlook Security Mode to "Enabled (Use Outlook Security Group Policy)".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.80 O365-OU-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The ability to demote attachments from Level 2 to Level 1 must be disabled.

```
GROUP ID: V-223360
RULE ID: SV-223360r961086
```

Rationale:

This policy setting controls whether Outlook users can demote attachments to Level 2 by using a registry key, which will allow them to save files to disk and open them from that location. Outlook uses two levels of security to restrict access to files attached to e-mail messages or other items. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.

If you enable this policy setting, users can create a list of Level 1 file types to demote to Level 2 by adding the file types to the following registry key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Security\Level1Remove.

If you disable or do not configure this policy setting, users cannot demote level 1 attachments to level 2, and the HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Security\Level1Remove registry key has no effect.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Attachment Security >> Allow users to demote attachments to Level 2 is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value allowuserstolowerattachments is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Attachment Security >> Allow users to demote attachments to Level 2 to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.81 O365-OU-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The display of Level 1 attachments must be disabled in Outlook.

```
GROUP ID: V-223361
RULE ID: SV-223361r961086
```

Rationale:

This policy setting controls whether Outlook blocks potentially dangerous attachments designated Level 1. Outlook uses two levels of security to restrict users' access to files attached to e-mail messages or other items. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.

If you enable this policy setting, Outlook users can gain access to Level 1 file type attachments by first saving the attachments to disk and then opening them, as with Level 2 attachments. If you disable this policy setting, Level 1 attachments do not display under any circumstances. If you do not configure this policy setting, Outlook completely blocks access to Level 1 files, and requires users to save Level 2 files to disk before opening them.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Attachment Security >> Display Level 1 attachments is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\outlook\security

If the value ShowLevel1Attach is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Attachment Security "Display Level 1 attachments" to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.82 O365-OU-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Level 1 file attachments must be blocked from being delivered.

```
GROUP ID: V-223362
RULE ID: SV-223362r961086
```

Rationale:

This policy setting controls whether Outlook users can demote attachments to Level 2 by using a registry key, which will allow them to save files to disk and open them from that location. Outlook uses two levels of security to restrict access to files attached to email messages or other items. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.

If you enable this policy setting, users can create a list of Level 1 file types to demote to Level 2 by adding the file types to the following registry key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security\Level1Remove.

If this policy setting is disabled or not configured, users cannot demote Level 1 attachments to Level 2, and the HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security\Level1Remove registry key has no effect.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Attachment Security >> Remove file extensions blocked as Level 1 is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security\FileExtensionsRemoveLevel1

If the registry key exists, this is a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Attachment Security >> Remove file extensions blocked as Level 1 to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.83 O365-OU-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Level 2 file attachments must be blocked from being delivered.

```
GROUP ID: V-223363
RULE ID: SV-223363r961086
```

Rationale:

This policy setting controls which types of attachments (determined by file extension) must be saved to disk before users can open them. Files with specific extensions can be categorized as Level 1 (users cannot view the file) or Level 2 (users can open the file after saving it to disk). Users can freely open files of types that are not categorized as Level 1 or Level 2.

If you enable this policy setting, you can specify a list of attachment file types to classify as Level 2, which forces users to actively decide to download the attachment to view it.

If you disable or do not configure this policy setting, Outlook does not classify any file type extensions as Level 2.

Important: This policy setting only applies if the "Outlook Security Mode" policy setting under "Microsoft Outlook 2016\Security\Security Form Settings" is configured to "Use Outlook Security Group Policy".

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Attachment Security >> Remove file extensions blocked as Level 2 is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security\FileExtensionsRemoveLevel2

If the registry key exists, this is a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Attachment Security >> Remove file extensions blocked as Level 2 to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.84 O365-OU-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Outlook must be configured to not run scripts in forms in which the script and the layout are contained within the message.

```
GROUP ID: V-223364
RULE ID: SV-223364r961092
```

Rationale:

This policy setting controls whether scripts can run in Outlook forms in which the script and layout are contained within the message. If you enable this policy setting, scripts can run in one-off Outlook forms. If you disable or do not configure this policy setting, Outlook does not run scripts in forms in which the script and the layout are contained within the message. Important: This policy setting only applies if the "Outlook Security Mode" policy setting under "Microsoft Outlook 2016\Security\Security Form Settings" is configured to "Use Outlook Security Group Policy".

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Custom Form Security "Allow scripts in one-off Outlook forms" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\outlook\security

If the value EnableOneOffFormScripts is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Custom Form Security "Allow scripts in one-off Outlook forms" to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.85 O365-OU-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When a custom action is executed that uses the Outlook object model, Outlook must automatically deny it.

```
GROUP ID: V-223365
RULE ID: SV-223365r961779
```

Rationale:

This policy setting controls whether Outlook prompts users before executing a custom action. Custom actions add functionality to Outlook that can be triggered as part of a rule. Among other possible features, custom actions can be created that reply to messages in ways that circumvent the Outlook model's programmatic send protections. If this policy is enabled, four options are available to control how Outlook functions when a custom action is executed that uses the Outlook object model:

- Prompt User
- Automatically Approve
- Automatically Deny
- Prompt user based on computer security. This option enforces the default configuration in Outlook.

If this policy is disabled or not configured, when Outlook or another program initiates a custom action using the Outlook object model, users are prompted to allow or reject the action. If this configuration is changed, malicious code can use the Outlook object model to compromise sensitive information or otherwise cause data and computing resources to be at risk. This is the equivalent of choosing Enabled -- Prompt user based on computer security.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Custom Form Security >> Set Outlook object model custom actions execution prompt is set to "Enabled" and "Automatically Deny".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for "promptoomcustomaction" is set to "REG_DWORD = 0", this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Custom Form Setting >> Set Outlook object model custom actions execution prompt to "Enabled" and select "Automatically Deny".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.86 O365-OU-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When an untrusted program attempts to programmatically access an Address Book using the Outlook object model, Outlook must automatically deny it.

```
GROUP ID: V-223366
RULE ID: SV-223366r961779
```

Rationale:

This policy setting controls what happens when an untrusted program attempts to gain access to an Address Book using the Outlook object model.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to programmatically access an Address Book using the Outlook object model:

- Prompt user - Users are prompted to approve every access attempt.
- Automatically approve - Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.
- Automatically deny - Outlook will automatically deny programmatic access requests from any program.
- Prompt user based on computer security - Outlook will rely on the setting in the "Programmatic Access" section of the Trust Center. This is the default behavior.

If you disable or do not configure this policy setting, when an untrusted application attempts to access the address book programmatically, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when accessing an address book is set to "Enabled (Automatically Deny)".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for promptoomaddressbookaccess is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when accessing an address book to "Enabled (Automatically Deny)".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.87 O365-OU-000022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When a user designs a custom form in Outlook and attempts to bind an Address Information field to a combination or formula custom field, Outlook must automatically deny it.

```
GROUP ID: V-223367
RULE ID: SV-223367r961779
```

Rationale:

This policy setting controls what happens when a user designs a custom form in Outlook and attempts to bind an Address Information field to a combination or formula custom field. If you enable this policy setting, you can choose from four different options when an untrusted program attempts to access address information using the UserProperties. Find method of the Outlook object model:

- Prompt user. The user will be prompted to approve every access attempt. - Automatically approve. Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.
- Automatically deny. Outlook will automatically deny programmatic access requests from any program.
- Prompt user based on computer security. Outlook will only prompt users when antivirus software is out of date or not running.

If you disable or do not configure this policy setting, when a user tries to bind an address information field to a combination or formula custom field in a custom form, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when accessing the Formula property of a UserProperty object is set to "Enabled (Automatically Deny)".

Use the Windows Registry to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\outlook\security

If the value PromptOOMFormulaAccess is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt When accessing the Formula property of a UserProperty object to "Enabled (Automatically Deny)".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.88 O365-OU-000023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When an untrusted program attempts to use the Save As command to programmatically save an item, Outlook must automatically deny it.

```
GROUP ID: V-223368
RULE ID: SV-223368r961779
```

Rationale:

This policy setting controls what happens when an untrusted program attempts to use the Save As command to programmatically save an item.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to use the Save As command to programmatically save an item:

- Prompt user. The user will be prompted to approve every access attempt.
- Automatically approve. Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.
- Automatically deny. Outlook will automatically deny programmatic access requests from any program.
- Prompt user based on computer security. Outlook will only prompt users when antivirus software is out of date or not running. This is the default configuration.

If you disable or do not configure this policy setting, when an untrusted application attempts to use the Save As command, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when executing Save As is set to "Enabled (Automatically Deny)".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for promptoomsaveas is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when executing Save As to "Enabled (Automatically Deny)".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.89 O365-OU-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When an untrusted program attempts to gain access to a recipient field, such as the, To: field, using the Outlook object model, Outlook must automatically deny it.

```
GROUP ID: V-223369
RULE ID: SV-223369r961779
```

Rationale:

This policy setting controls what happens when an untrusted program attempts to gain access to a recipient field, such as the "To:" field, using the Outlook object model.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to access a recipient field using the Outlook object model:

- Prompt user. The user will be prompted to approve every access attempt.
- Automatically approve. Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.
- Automatically deny. Outlook will automatically deny programmatic access requests from any program.
- Prompt user based on computer security. Outlook will only prompt users when antivirus software is out of date or not running. This is the default configuration.

If you disable or do not configure this policy setting, when an untrusted application attempts to access recipient fields, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when reading address information is set to "Enabled (Automatically Deny)".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for promptoomaddressinformationaccess is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when reading address information to "Enabled (Automatically Deny)".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.90 O365-OU-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When an untrusted program attempts to programmatically send e-mail in Outlook using the Response method of a task or meeting request, Outlook must automatically deny it.

```
GROUP ID: V-223370
RULE ID: SV-223370r961779
```

Rationale:

This policy setting controls what happens when an untrusted program attempts to programmatically send e-mail in Outlook using the Response method of a task or meeting request.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to programmatically send e-mail using the Response method of a task or meeting request:

- Prompt user. The user will be prompted to approve every access attempt.
- Automatically approve. Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.
- Automatically deny. Outlook will automatically deny programmatic access requests from any program.
- Prompt user based on computer security. Outlook only prompts users when antivirus software is out of date or not running. This is the default configuration.

If you disable or do not configure this policy setting, when an untrusted application attempts to respond to tasks or meeting requests programmatically, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when responding to meeting and task requests is set to "Enabled (Automatically Deny)"

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for promptoommeetingtaskrequestresponse is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when responding to meeting and task requests to "Enabled (Automatically Deny)".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.91 O365-OU-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

When an untrusted program attempts to send e-mail programmatically using the Outlook object model, Outlook must automatically deny it.

```
GROUP ID: V-223371
RULE ID: SV-223371r961779
```

Rationale:

This policy setting controls what happens when an untrusted program attempts to send e-mail programmatically using the Outlook object model.

If you enable this policy setting, you can choose from four different options when an untrusted program attempts to send e-mail programmatically using the Outlook object model:

- Prompt user - The user will be prompted to approve every access attempt.
- Automatically approve - Outlook will automatically grant programmatic access requests from any program. This option can create a significant vulnerability, and is not recommended.
- Automatically deny - Outlook will automatically deny programmatic access requests from any program.
- Prompt user based on computer security. Outlook will only prompt users when antivirus software is out of date or not running.

Important: This policy setting only applies if the "Outlook Security Mode" policy setting under "Microsoft Outlook 2016\Security\Security Form Settings" is configured to "Use Outlook Security Group Policy".

If you disable or do not configure this policy setting, when an untrusted application attempts to send mail programmatically, Outlook relies on the setting configured in the "Programmatic Access" section of the Trust Center.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when sending mail is set to "Enabled (Automatically Deny)".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for promptoomsend is set to REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Security Form Settings >> Programmatic Security >> Configure Outlook object model prompt when sending mail to "Enabled (Automatically Deny)".

Additional Information:

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.92 O365-OU-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Outlook must be configured to not allow hyperlinks in suspected phishing messages.

```
GROUP ID: V-223372
RULE ID: SV-223372r961863
```

Rationale:

This policy setting controls whether hyperlinks in suspected phishing e-mail messages in Outlook are allowed. If you enable this policy setting, Outlook will allow hyperlinks in suspected phishing messages that are not also classified as junk e-mail. If you disable or do not configure this policy setting, Outlook will not allow hyperlinks in suspected phishing messages, even if they are not classified as junk e-mail.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Trust Center "Allow hyperlinks in suspected phishing e-mail messages" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\outlook\options\mail

If the value JunkMailEnableLinks is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Trust Center "Allow hyperlinks in suspected phishing e-mail messages" to "Disabled".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.93 O365-OU-000028 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Security Level for macros in Outlook must be configured to Warn for signed and disable unsigned.

```
GROUP ID: V-223373
RULE ID: SV-223373r961086
```

Rationale:

This policy setting controls the security level for macros in Outlook.

If you enable this policy setting, you can choose from four options for handling macros in Outlook:

- Always warn. This option corresponds to the "Warnings for all macros" option in the "Macro Security" section of the Outlook Trust Center. Outlook disables all macros that are not opened from a trusted location, even if the macros are signed by a trusted publisher. For each disabled macro, Outlook displays a security alert dialog box with information about the macro and its digital signature (if present), and allows users to enable the macro or leave it disabled.
- Never warn, disable all. This option corresponds to the "No warnings and disable all macros" option in the Trust Center. Outlook disables all macros that are not opened from trusted locations, and does not notify users.
- Warning for signed, disable unsigned. This option corresponds to the "Warnings for signed macros; all unsigned macros are disabled" option in the Trust Center. Outlook handles macros as follows: --If a macro is digitally signed by a trusted publisher, the macro can run if the user has already trusted the publisher. --If a macro has a valid signature from a publisher that the user has not trusted, the security alert dialog box for the macro lets the user choose whether to enable the macro for the current session, disable the macro for the current session, or to add the publisher to the Trusted Publishers list so that it will run without prompting the user in the future. --If a macro does not have a valid signature, Outlook disables it without prompting the user, unless it is opened from a trusted location. This option is the default configuration in Outlook.
- No security check. This option corresponds to the "No security check for macros (Not recommended)" option in the Trust Center. Outlook runs all macros without prompting users. This configuration makes users' computers vulnerable to potentially malicious code and is not recommended.

If you disable or do not configure this policy setting, the behavior is the equivalent of Enabled -- Warning for signed, disable unsigned.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Trust Center >> Security setting for macros must be set to "Enabled: Warn for signed, disable unsigned".

Use the Windows Registry to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\outlook\security

If the value for level is set to REG_DWORD = 3, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Outlook 2016 >> Security >> Trust Center >> Security setting for macros must to "Enabled: Warn for signed, disable unsigned".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.94 O365-PR-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Trusted Locations on the network must be disabled in Project.

```
GROUP ID: V-223374
RULE ID: SV-223374r961092
```

Rationale:

This policy setting controls whether trusted locations on the network can be used.

If you enable this policy setting, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by clicking the "Add new location" button in the Trusted Locations section of the Trust Center. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

If you disable this policy setting, the selected application ignores any network locations listed in the Trusted Locations section of the Trust Center.

If you also deploy Trusted Locations via Group Policy, you should verify whether any of them are remote locations. If any of them are remote locations and you do not allow remote locations via this policy setting, those policy keys that point to remote locations will be ignored on client computers.

Disabling this policy setting does not delete any network locations from the Trusted Locations list, but causes disruption for users who add network locations to the Trusted Locations list. Users are also prevented from adding new network locations to the Trusted Locations list in the Trust Center. We recommended that you do not enable this policy setting as the "Allow Trusted Locations on my network (not recommended)" check box also states. Therefore, in practice, it should be possible to disable this policy setting in most situations without causing significant usability issues for most users.

If you do not enable this policy setting, users can select the "Allow Trusted Locations on my network (not recommended)" check box if desired and then specify trusted locations by clicking the "Add new location" button.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Project 2016 >> Project Options >> Security >> Trust Center >> Allow Trusted Locations on the network is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\ms project\security\trusted locations

If the value allownetworklocations is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Project 2016 >> Project Options >> Security >> Trust Center >> Allow Trusted Locations on the network to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.95 O365-PR-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Project must automatically disable unsigned add-ins without informing users.

```
GROUP ID: V-223375
RULE ID: SV-223375r1016169
```

Rationale:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if the "Require that application add-ins are signed by Trusted Publisher" policy setting is enabled, which prevents users from changing this policy setting.

If this policy setting is enabled, applications automatically disable unsigned add-ins without informing users.

If this policy setting is disabled, if this application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If this policy setting is not configured, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Project 2016 >> Project Options >> Security >> Trust Center >> "Disable Trust Bar Notification for unsigned application add-ins and block them" is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\ms project\security

If the value notbpromptunsignedaddin is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Project 2016 >> Project Options >> Security >> Trust Center >> "Disable Trust Bar Notification for unsigned application add-ins and block them" to "Enabled".

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.96 O365-PR-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VBA Macros not digitally signed must be blocked in Project.

```
GROUP ID: V-223376
RULE ID: SV-223376r960963
```

Rationale:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If you enable this policy setting, you can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office. This option also allows users to potentially enable unsigned/untrusted macros. If a site requires the use of macros, they must be signed /approved and added to appropriate locations listed in the Trust Center Settings.
- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.
- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.
- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

If you disable this policy setting, "Disable all with notification" will be the default setting.

If you do not configure this policy setting, when users open files in the specified applications that contain VBA macros, the applications open the files with the macros disabled and display the Trust Bar with a warning that macros are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content", then the document is added as a trusted document.

Important: If "Disable all except digitally signed macros" is selected, users will not be able to open unsigned Access databases.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Project 2016 >> Project Options >> Security >> Trust Center >> VBA Macro Notification Settings is set to "Enabled" "Disable all except digitally signed macros".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\ms project\security

If the value for vbawarnings is REG_DWORD = 3, this is not a finding. A value of REG_DWORD = 4 is also acceptable. If the registry key does not exist or is not configured properly, this is a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Project 2016 >> Project Options >> Security >> Trust Center >> VBA Macro Notification Settings to "Enabled" "Disable all except digitally signed macros".

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.97 O365-PT-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VBA Macros not digitally signed must be blocked in PowerPoint.

```
GROUP ID: V-223377
RULE ID: SV-223377r960963
```

Rationale:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If you enable this policy setting, you can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office. This option also allows users to potentially enable unsigned/untrusted macros. If a site requires the use of macros, they must be signed /approved and added to appropriate locations listed in the Trust Center Settings.
- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.
- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.
- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

If you disable this policy setting, "Disable all with notification" will be the default setting.

If you do not configure this policy setting, when users open files in the specified applications that contain VBA macros, the applications open the files with the macros disabled and display the Trust Bar with a warning that macros are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content", then the document is added as a trusted document.

Important: If "Disable all except digitally signed macros" is selected, users will not be able to open unsigned Access databases.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> VBA Macro Notification Settings is set to "Enabled" "Disable all except digitally signed macros".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\powerpoint\security

If the value for vbawarnings is REG_DWORD = 3 this is not a finding. A value of REG_DWORD = 4 is also acceptable. If the registry key does not exist or is not configured properly, this is a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> VBA Macro Notification Settings to "Enabled" "Disable all except digitally signed macros".

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.98 O365-PT-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The ability to run programs from PowerPoint must be disabled.

```
GROUP ID: V-223378
RULE ID: SV-223378r961092
```

Rationale:

This policy setting controls the prompting and activation behavior for the "Run Programs" option for action buttons in PowerPoint.

If you enable this policy setting, you can choose from three options to control how the "Run Programs" option functions:

- Disable (do not run any programs). If users click an action button with the "Run Programs" action assigned to it, nothing will happen. This option enforces the default configuration in PowerPoint.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Run Programs is set to "Enabled" "Disable (do not run any programs)".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\powerpoint\security

If the value runprograms does not exist, this is not a finding. If the value is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Run Programs to "Enabled" "Disable (do not run any programs)".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.99 O365-PT-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of PowerPoint 97-2003 presentations, shows, templates, and add-in files must be blocked.

```
GROUP ID: V-223379
RULE ID: SV-223379r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save PowerPoint files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open, view, edit, or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> File Block Settings >> PowerPoint 97-2003 presentations, shows, templates and add-in files is set to "Enabled" "Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\powerpoint\security\fileblock

If the value for binaryfiles is set to REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> File Block Settings >> PowerPoint 97-2003 presentations, shows, templates and add-in files to "Enabled" "Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.100 O365-PT-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The default file block behavior must be set to not open blocked files in PowerPoint.

```
GROUP ID: V-223380
RULE ID: SV-223380r961086
```

Rationale:

This policy setting allows you to determine if users can open, view, or edit Word files. If you enable this policy setting, you can set one of these options:

- Blocked files are not opened.
- Blocked files open in Protected View and cannot be edited.
- Blocked files open in Protected View and can be edited.

If you disable or do not configure this policy setting, the behavior is the same as the "Blocked files are not opened" setting. Users will not be able to open blocked files.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> File Block Settings "Set default file block behavior" is set to "Enabled: Blocked files are not opened".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\security\fileblock

If the value OpenInProtectedView is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> File Block Settings "Set default file block behavior" to "Enabled: Blocked files are not opened".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)

- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.101 O365-PT-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Encrypted macros in PowerPoint Open XML presentations must be scanned.

```
GROUP ID: V-223381
RULE ID: SV-223381r961092
```

Rationale:

This policy setting controls whether encrypted macros in Open XML presentations are required to be scanned with anti-virus software before being opened. If you enable this policy setting, you may choose one of these options:

- Scan encrypted macros: Encrypted macros are disabled unless anti-virus software is installed. Encrypted macros are scanned by your anti-virus software when you attempt to open an encrypted presentation that contains macros.
- Scan if anti-virus software available: If anti-virus software is installed, scan the encrypted macros first before allowing them to load. If anti-virus software is not available, allow encrypted macros to load.
- Load macros without scanning: Do not check for anti-virus software and allow macros to be loaded in an encrypted file. If you disable or do not configure this policy setting, the behavior will be similar to the "Scan encrypted macros" option.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security "Scan encrypted macros in PowerPoint Open XML presentations" is set to "Enabled" and "Scan encrypted macros".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\security

If the value PowerPointBypassEncryptedMacroScan does not exist, this is not a finding.

If the value is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security "Scan encrypted macros in PowerPoint Open XML presentations" to "Enabled" and "Scan encrypted macros".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.102 O365-PT-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

File validation in PowerPoint must be enabled.

```
GROUP ID: V-223382
RULE ID: SV-223382r961092
```

Rationale:

This policy setting allows you to turn off the file validation feature. If you enable this policy setting, file validation will be turned off. If you disable or do not configure this policy setting, file validation will be turned on. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security "Turn off file validation" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\security\filevalidation

If the value EnableOnLoad is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security "Turn off file validation" to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.103 O365-PT-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Macros from the Internet must be blocked from running in PowerPoint.

```
GROUP ID: V-223383
RULE ID: SV-223383r961092
```

Rationale:

This policy setting allows you to block macros from running in Office files that come from the Internet. If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to "Enable Content", users will receive a notification that macros are blocked from running.

If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run. If you disable or do not configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center "Block macros from running in Office files from the Internet" is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\powerpoint\security

If the value blockcontentexecutionfrominternet is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center "Block macros from running in Office files from the Internet" to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)

- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.104 O365-PT-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Unsigned add-ins in PowerPoint must be blocked with no Trust Bar Notification to the user.

```
GROUP ID: V-223384
RULE ID: SV-223384r1016170
```

Rationale:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if the "Require that application add-ins are signed by Trusted Publisher" policy setting is enabled, which prevents users from changing this policy setting.

If this policy setting is enabled, applications automatically disable unsigned add-ins without informing users.

If this policy setting is disabled, if this application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If this policy setting is not configured, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center "Disable Trust Bar Notification for unsigned application add-ins and block them" is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\powerpoint\security

If the value notbpromptunsignedaddin is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center "Disable Trust Bar Notification for unsigned application add-ins and block them" to "Enabled".

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.105 O365-PT-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files downloaded from the Internet must be opened in Protected view in PowerPoint.

```
GROUP ID: V-223385
RULE ID: SV-223385r961086
```

Rationale:

This policy setting allows you to determine if files downloaded from the Internet zone open in Protected View. If you enable this policy setting, files downloaded from the Internet zone do not open in Protected View. If you disable or do not configure this policy setting, files downloaded from the Internet zone open in Protected View.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Protected View "Do not open files from the Internet zone in Protected View" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\security\protectedview

If the value DisableInternetFilesInPV is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Protected View "Do not open files from the Internet zone in Protected View" to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.106 O365-PT-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

PowerPoint attachments opened from Outlook must be in Protected View.

```
GROUP ID: V-223386
RULE ID: SV-223386r961086
```

Rationale:

This policy setting allows for determining whether PowerPoint files in Outlook attachments open in Protected View. If enabling this policy setting, Outlook attachments do not open in Protected View. If disabling or not configuring this policy setting, Outlook attachments open in Protected View.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Protected View "Turn off Protected View for attachments opened from Outlook" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\security\protectedview

If the value DisableAttachmentsInPV is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Protected View "Turn off Protected View for attachments opened from Outlook" to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.107 O365-PT-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files in unsafe locations must be opened in Protected view in PowerPoint.

```
GROUP ID: V-223387
RULE ID: SV-223387r961086
```

Rationale:

This policy setting determines whether files located in unsafe locations will open in Protected View. If unsafe locations have not been specified, only the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations. If enabling this policy setting, files located in unsafe locations do not open in Protected View. If disabling or not configuring this policy setting, files located in unsafe locations open in Protected View.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Protected View "Do not open files in unsafe locations in Protected View" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\security\protectedview

If the value DisableUnsafeLocationsInPV is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Protected View "Do not open files in unsafe locations in Protected View" to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.108 O365-PT-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If file validation fails, files must be opened in Protected view in PowerPoint with ability to edit disabled.

```
GROUP ID: V-223388
RULE ID: SV-223388r961092
```

Rationale:

This policy setting controls how Office handles documents when they fail file validation. If you enable this policy setting, you can configure the following options for files that fail file validation:

- Block files completely. Users cannot open the files.
- Open files in Protected View and disallow edit. Users cannot edit the files. This is also how Office handles the files if you disable this policy setting.
- Open files in Protected View and allow edit. Users can edit the files. This is also how Office handles the files if you do not configure this policy setting.

If you disable this policy setting, Office follows the "Open files in Protected View and disallow edit" behavior. If you do not configure this policy setting, Office follows the "Open files in Protected View and allow edit" behavior.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Protected View >> Set document behavior if file validation fails is set to "Enabled: Open in Protected View". Verify the check box for "Allow edit" is not selected.

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\security\filevalidation

If the value openinprotectedview does not exist, this is not a finding.

If both the value for openinprotectedview is REG_DWORD = 1 and the value for DisableEditFromPV is set to REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Protected View >> Set document behavior if file validation fails to "Enabled: Open in Protected View".

Uncheck the "Allow edit" check box.

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.109 O365-PT-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The use of network locations must be ignored in PowerPoint.

```
GROUP ID: V-223389
RULE ID: SV-223389r961092
```

Rationale:

This policy setting controls whether trusted locations on the network can be used. If you enable this policy setting, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by clicking the "Add new location" button in the Trusted Locations section of the Trust Center. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

If you disable this policy setting, the selected application ignores any network locations listed in the Trusted Locations section of the Trust Center. If you also deploy Trusted Locations via Group Policy, you should verify whether any of them are remote locations. If any of them are remote locations and you do not allow remote locations via this policy setting, those policy keys that point to remote locations will be ignored on client computers.

Disabling this policy setting does not delete any network locations from the Trusted Locations list, but causes disruption for users who add network locations to the Trusted Locations list. Users are also prevented from adding new network locations to the Trusted Locations list in the Trust Center. It is recommended that you do not enable this policy setting, as the "Allow Trusted Locations on my network (not recommended) check box also states. Therefore, in practice, it should be possible to disable this policy setting in most situations without causing significant usability issues for most users. If you do not enable this policy setting, users can select the "Allow Trusted Locations on my network (not recommended)" check box if desired and then specify trusted locations by clicking the "Add new location" button.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Trusted Locations "Allow Trusted Locations on the network" is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\security\trusted locations

If the value AllowNetworkLocations is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft PowerPoint 2016 >> PowerPoint Options >> Security >> Trust Center >> Trusted Locations "Allow Trusted Locations on the network" to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.110 O365-PU-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Publisher must be configured to prompt the user when another application programmatically opens a macro.

```
GROUP ID: V-223390
RULE ID: SV-223390r961086
```

Rationale:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if you enable the "Require that application add-ins are signed by Trusted Publisher" policy setting, which prevents users from changing this policy setting.

If you enable this policy setting, applications automatically disable unsigned add-ins without informing users.

If you disable this policy setting, if this application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If you do not configure this policy setting, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Publisher 2016 >> Security >> Publisher Automation Security Level is set to "Enabled" "By UI (prompted)".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\common\security

If the value automationsecuritypublisher is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Publisher 2016 >> Security >> Publisher Automation Security Level to "Enabled" "By UI (prompted)"

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.111 O365-PU-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Publisher must automatically disable unsigned add-ins without informing users.

```
GROUP ID: V-223391
RULE ID: SV-223391r1016171
```

Rationale:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if the "Require that application add-ins are signed by Trusted Publisher" policy setting is enabled, which prevents users from changing this policy setting.

If this policy setting is enabled, applications automatically disable unsigned add-ins without informing users.

If this policy setting is disabled, if this application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If this policy setting is not configured, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Publisher 2016 >> Security >> Trust Center >> Disable Trust Bar Notification for unsigned application add-ins is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\publisher\security

If the value notbpromptunsignedaddin is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Publisher 2016 >> Security >> Trust Center >> Disable Trust Bar Notification for unsigned application add-ins to "Enabled".

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.112 O365-PU-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Publisher must disable all unsigned VBA macros.

```
GROUP ID: V-223392
RULE ID: SV-223392r1016172
```

Rationale:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If this policy setting is enabled, users can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office. This option also allows users to potentially enable unsigned/untrusted macros. If a site requires the use of macros, they must be signed/approved and added to appropriate locations listed in the Trust Center Settings.
- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.
- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.
- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

If this policy setting is disabled, "Disable all with notification" will be the default setting.

If this policy setting is not configured, when users open files in the specified applications that contain VBA macros, the applications open the files with the macros disabled and display the Trust Bar with a warning that macros are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content", then the document is added as a trusted document.

Important: If "Disable all except digitally signed macros" is selected, users will not be able to open unsigned Access databases.

Audit:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Publisher 2016 >> Security >> Trust Center >> VBA Macro Notification Settings >> VBA Macro Notification Settings to "Enabled" "Disable all except digitally signed macros".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\publisher\security

If the value vbawarnings is REG_DWORD = 3, this is not a finding. A value of REG_DWORD = 4 is also acceptable. If the registry key does not exist or is not configured properly, this is a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Publisher 2016 >> Security >> Trust Center >> VBA Macro Notification Settings >> VBA Macro Notification Settings must be set to "Enabled" and "Disable all except digitally signed macros".

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.113 O365-VI-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VBA Macros not digitally signed must be blocked in Visio.

```
GROUP ID: V-223393
RULE ID: SV-223393r960963
```

Rationale:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If you enable this policy setting, you can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office. This option also allows users to potentially enable unsigned/untrusted macros. If a site requires the use of macros, they must be signed /approved and added to appropriate locations listed in the Trust Center Settings.
- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.
- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.
- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

If you disable this policy setting, "Disable all with notification" will be the default setting.

If you do not configure this policy setting, when users open files in the specified applications that contain VBA macros, the applications open the files with the macros disabled and display the Trust Bar with a warning that macros are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content", then the document is added as a trusted document.

Important: If "Disable all except digitally signed macros" is selected, users will not be able to open unsigned Access databases.

Audit:

Verify the policy value for User Configuration >> Administrative Templates/Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> VBA Macro Notification Settings is set to "Enabled" and "Disable all except digitally signed macros".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\visio\security

If the value for vbawarnings is REG_DWORD = 3, this is not a finding. A value of REG_DWORD = 4 is also acceptable. If the registry key does not exist or is not configured properly, this is a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates/Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> VBA Macro Notification Settings to "Enabled" and select "Disable all except digitally signed macros".

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.114 O365-VI-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Trusted Locations on the network must be disabled in Visio.

```
GROUP ID: V-223394
RULE ID: SV-223394r961092
```

Rationale:

This policy setting controls whether trusted locations on the network can be used.

If you enable this policy setting, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by clicking the "Add new location" button in the Trusted Locations section of the Trust Center. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

If you disable this policy setting, the selected application ignores any network locations listed in the Trusted Locations section of the Trust Center.

If you also deploy Trusted Locations via Group Policy, you should verify whether any of them are remote locations. If any of them are remote locations and you do not allow remote locations via this policy setting, those policy keys that point to remote locations will be ignored on client computers.

Disabling this policy setting does not delete any network locations from the Trusted Locations list, but causes disruption for users who add network locations to the Trusted Locations list. Users are also prevented from adding new network locations to the Trusted Locations list in the Trust Center. We recommended that you do not enable this policy setting as the "Allow Trusted Locations on my network (not recommended)" check box also states. Therefore, in practice, it should be possible to disable this policy setting in most situations without causing significant usability issues for most users.

If you do not enable this policy setting, users can select the "Allow Trusted Locations on my network (not recommended)" check box if desired and then specify trusted locations by clicking the "Add new location" button.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> Allow Trusted Locations on the network is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\visio\security\trusted locations

If the value for allownetworklocations is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> Allow Trusted Locations on the network to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.115 O365-VI-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Visio must automatically disable unsigned add-ins without informing users.

```
GROUP ID: V-223395
RULE ID: SV-223395r1016173
```

Rationale:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if the "Require that application add-ins are signed by Trusted Publisher" policy setting is enabled, which prevents users from changing this policy setting.

If this policy setting is enabled, applications automatically disable unsigned add-ins without informing users.

If this policy setting is disabled, if this application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If this policy setting is not configured, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> Disable Trust Bar Notification for unsigned application add-ins and block them is set to Enabled.

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\visio\security

If the value notbpromptunsignedaddin is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> Disable Trust Bar Notification for unsigned application add-ins and block them to Enabled.

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.116 O365-VI-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Visio 2000-2002 Binary Drawings, Templates and Stencils must be blocked.

```
GROUP ID: V-223396
RULE ID: SV-223396r961086
```

Rationale:

This policy setting allows you to determine whether users can open or save Visio files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

-Do not block: The file type will not be blocked. -Save blocked: Saving of the filet type will be blocked. -Open/Save blocked: Both opening and saving of the file type will be blocked.

If you disable or do not configure this policy setting, the file type will be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> File Block Settings "Visio 2000-2002 Binary Drawings, Templates and Stencils" is set to "Enabled" and "Open/Save blocked".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\visio\security\fileblock

If the value "visio2000files" is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> File Block Settings "Visio 2000-2002 Binary Drawings, Templates and Stencils" to "Enabled" and "Open/Save blocked".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.117 O365-VI-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Visio 2003-2010 Binary Drawings, Templates and Stencils must be blocked.

```
GROUP ID: V-223397
RULE ID: SV-223397r961086
```

Rationale:

This policy setting allows you to determine whether users can open or save Visio files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

-Do not block: The file type will not be blocked. -Save blocked: Saving of the filet type will be blocked. -Open/Save blocked: Both opening and saving of the file type will be blocked.

If you disable or do not configure this policy setting, the file type will be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> File Block Settings "Visio 2003-2010 Binary Drawings, Templates and Stencils" is set to "Enabled" and "Open/Save blocked".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\visio\security\fileblock

If the value "visio2003files" is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> File Block Settings "Visio 2003-2010 Binary Drawings, Templates and Stencils" to "Enabled" and "Open/Save blocked".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.118 O365-VI-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Visio 5.0 or earlier Binary Drawings, Templates and Stencils must be blocked.

```
GROUP ID: V-223398
RULE ID: SV-223398r961086
```

Rationale:

This policy setting allows you to determine whether users can open or save Visio files with the format specified by the title of this policy setting.

If you enable this policy setting, you can specify whether users can open or save files.

The options that can be selected are below. Note: Not all options may be available for this policy setting.

-Do not block: The file type will not be blocked. -Save blocked: Saving of the filet type will be blocked. -Open/Save blocked: Both opening and saving of the file type will be blocked.

If you disable or do not configure this policy setting, the file type will be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> File Block Settings "Visio 5.0 or earlier Binary Drawings, Templates and Stencils" is set to "Enabled" and "Open/Save blocked".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\visio\security\fileblock

If the value "visio50andearlierfiles" is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> File Block Settings "Visio 5.0 or earlier Binary Drawings, Templates and Stencils" to "Enabled" and "Open/Save blocked".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.119 O365-VI-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Macros must be blocked from running in Visio files from the Internet.

```
GROUP ID: V-223399
RULE ID: SV-223399r961092
```

Rationale:

This policy setting allows you to block macros from running in Office files that come from the Internet.

If you enable this policy setting, macros are blocked from running, even if “Enable all macros” is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to “Enable Content”, users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

If you disable or do not configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> Block macros from running in Office files from the Internet is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\visio\security

If the value blockcontentexecutionfrominternet is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Visio 2016 >> Visio Options >> Security >> Trust Center >> Block macros from running in Office files from the Internet to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.120 O365-WD-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Word must automatically disable unsigned add-ins without informing users.

```
GROUP ID: V-223400
RULE ID: SV-223400r1016174
```

Rationale:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if the "Require that application add-ins are signed by Trusted Publisher" policy setting is enabled, which prevents users from changing this policy setting.

If this policy setting is enabled, applications automatically disable unsigned add-ins without informing users.

If this policy setting is disabled, if this application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If this policy setting is not configured, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Disable Trust Bar Notification for unsigned application add-ins and block them is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\word\security

If the value for notbpromptunsignedaddin is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Disable Trust Bar Notification for unsigned application add-ins and block them to "Enabled".

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

1.121 O365-WD-000002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

In Word, encrypted macros must be scanned.

```
GROUP ID: V-223401
RULE ID: SV-223401r961092
```

Rationale:

This policy setting controls whether encrypted macros in Open XML documents be are required to be scanned with anti-virus software before being opened.

If you enable this policy setting, you may choose one of these options:

- Scan encrypted macros: encrypted macros are disabled unless anti-virus software is installed. Encrypted macros are scanned by your anti-virus software when you attempt to open an encrypted workbook that contains macros.
- Scan if anti-virus software available: if anti-virus software is installed, scan the encrypted macros first before allowing them to load. If anti-virus software is not available, allow encrypted macros to load.
- Load macros without scanning: do not check for anti-virus software and allow macros to be loaded in an encrypted file.

If you disable or do not configure this policy setting, the behavior will be similar to the "Scan encrypted macros" option.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Scan encrypted macros in Word Open XML documents is set to "Enabled" "Scan encrypted macros (default)".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\word\security

If the value WordBypassEncryptedMacroScan does not exist, this is not a finding. If the value is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Scan encrypted macros in Word Open XML documents to "Enabled" "Scan encrypted macros (default)".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.122 O365-WD-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files downloaded from the Internet must be opened in Protected view in Word.

```
GROUP ID: V-223402
RULE ID: SV-223402r961086
```

Rationale:

This policy setting allows you to determine if files downloaded from the Internet zone open in Protected View.

If you enable this policy setting, files downloaded from the Internet zone do not open in Protected View.

If you disable or do not configure this policy setting, files downloaded from the Internet zone open in Protected View.

Audit:

Verify the policy setting, User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Protected View >> Do not open files from the Internet zone in Protected View is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\word\security\protectedview

If the value for disableinternetfilesinpv is REG_DWORD = 0, this is not a finding. If the value does not exist, this is not a finding.

If the value is REG_DWORD = 1, this is a finding.

Remediation:

Set the policy setting, User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Protected View >> Do not open files from the Internet zone in Protected View to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)

- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.123 O365-WD-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Files located in unsafe locations must be opened in Protected view in Word.

```
GROUP ID: V-223403
RULE ID: SV-223403r961086
```

Rationale:

This policy setting lets you determine if files located in unsafe locations will open in Protected View. If you have not specified unsafe locations, only the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations.

If you enable this policy setting, files located in unsafe locations do not open in Protected View.

If you disable or do not configure this policy setting, files located in unsafe locations open in Protected View.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Protected View >> Do not open files in unsafe locations in Protected View is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\word\security\protectedview.

If the value for disableunsafelocationsinpv is REG_DWORD = 0, this is not a finding. If the value does not exist, this is not a finding.

If the value is REG_DWORD = 1, this is a finding.

Remediation:

Set the policy setting, User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Protected View >> Do not open files in unsafe locations in Protected View to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)

- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.124 O365-WD-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If file validation fails, files must be opened in Protected view in Word with ability to edit disabled.

```
GROUP ID: V-223404
RULE ID: SV-223404r961086
```

Rationale:

This policy setting controls how Office handles documents when they fail file validation.

If you enable this policy setting, you can configure the following options for files that fail file validation:

- Block files completely. Users cannot open the files.
- Open files in Protected View and disallow edit. Users cannot edit the files. This is also how Office handles the files if you disable this policy setting.
- Open files in Protected View and allow edit. Users can edit the files. This is also how Office handles the files if you do not configure this policy setting.

If you disable this policy setting, Office follows the "Open files in Protected View and disallow edit" behavior.

If you do not configure this policy setting, Office follows the "Open files in Protected View and allow edit" behavior.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Protected View >> Set document behavior if file validation fails is set to "Enabled: Open in Protected View". Verify the check box for "Allow edit" is not selected.

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\Word\security\filevalidation

If the value openinprotectedview does not exist, this is not a finding.

If both the value for openinprotectedview is REG_DWORD = 1 and the value for DisableEditFromPV is set to REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Protected View >> Set document behavior if file validation fails to "Enabled: Open in Protected View".

Uncheck the "Allow edit" check box.

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.125 O365-WD-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Word attachments opened from Outlook must be in Protected View.

```
GROUP ID: V-223405
RULE ID: SV-223405r961086
```

Rationale:

This policy setting allows you to determine if Word files in Outlook attachments open in Protected View.

If you enable this policy setting, Outlook attachments do not open in Protected View.

If you disable or do not configure this policy setting, Outlook attachments open in Protected View.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security>> Trust Center>> Protected View >> Turn off Protected View for attachments opened from Outlook is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\word\security\protectedview

If the value for disableattachmentsinpv is REG_DWORD = 0, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security>> Trust Center>> Protected View >> Turn off Protected View for attachments opened from Outlook to "Disabled".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.126 O365-WD-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The default file block behavior must be set to not open blocked files in Word.

```
GROUP ID: V-223406
RULE ID: SV-223406r961086
```

Rationale:

This policy setting allows you to determine if users can open, view, or edit Word files.

If you enable this policy setting, you can set one of these options:

- Blocked files are not opened.
- Blocked files open in Protected View and cannot be edited.
- Blocked files open in Protected View and can be edited.

If you disable or do not configure this policy setting, the behavior is the same as the "Blocked files are not opened" setting. Users will not be able to open blocked files.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Set default file block behavior" is set to "Enabled: Blocked files are not opened".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value OpenInProtectedView is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Set default file block behavior" to "Enabled: Blocked files are not opened".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)

- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.127 O365-WD-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of Word 2 and earlier binary documents and templates must be blocked.

```
GROUP ID: V-223407
RULE ID: SV-223407r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Word files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 2 and earlier binary documents and templates" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value Word2Files is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 2 and earlier binary documents and templates" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.128 O365-WD-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of Word 2000 binary documents and templates must be blocked.

```
GROUP ID: V-223408
RULE ID: SV-223408r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Word files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 2000 binary documents and templates" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value Word2000Files is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 2000 binary documents and templates" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.129 O365-WD-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of Word 2003 binary documents and templates must be blocked.

```
GROUP ID: V-223409
RULE ID: SV-223409r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Word files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 2003 binary documents and templates" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value word2003files is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 2003 binary documents and templates" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.130 O365-WD-000011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of Word 2007 and later binary documents and templates must be blocked.

```
GROUP ID: V-223410
RULE ID: SV-223410r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Word files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 2007 and later binary documents and templates" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value word2007files is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 2007 and later binary documents and templates" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.131 O365-WD-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of Word 6.0 binary documents and templates must be blocked.

```
GROUP ID: V-223411
RULE ID: SV-223411r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Word files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 6.0 binary documents and templates" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value word60files is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 6.0 binary documents and templates" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.132 O365-WD-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of Word 95 binary documents and templates must be blocked.

```
GROUP ID: V-223412
RULE ID: SV-223412r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Word files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 95 binary documents and templates" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value word95files is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 95 binary documents and templates" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.133 O365-WD-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of Word 97 binary documents and templates must be blocked.

```
GROUP ID: V-223413
RULE ID: SV-223413r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Word files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 97 binary documents and templates" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value word97files is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word 97 binary documents and templates" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.134 O365-WD-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Open/Save of Word XP binary documents and templates must be blocked.

```
GROUP ID: V-223414
RULE ID: SV-223414r961086
```

Rationale:

This policy setting allows you to determine whether users can open, view, edit, or save Word files with the format specified by the title of this policy setting. If you enable this policy setting, you can specify whether users can open, view, edit, or save files. The options that can be selected are below. Note: Not all options may be available for this policy setting.

- Do not block: The file type will not be blocked.
- Save blocked: Saving of the file type will be blocked.
- Open/Save blocked, use open policy: Both opening and saving of the file type will be blocked. The file will open based on the policy setting configured in the "default file block behavior" key.
- Block: Both opening and saving of the file type will be blocked, and the file will not open.
- Open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit the file type will not be enabled.
- Allow editing and open in Protected View: Both opening and saving of the file type will be blocked, and the option to edit will be enabled.

If you disable or do not configure this policy setting, the file type will not be blocked.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word XP binary documents and templates" is set to "Enabled: Open/Save blocked, use open policy".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security\fileblock

If the value wordxpfiles is REG_DWORD = 2, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> File Block Settings "Word XP binary documents and templates" to "Enabled: Open/Save blocked, use open policy".

Additional Information:

CCI-001662 Take organization-defined corrective action when organization-defined unacceptable mobile code is identified.

- NIST SP 800-53::SC-18 (1)
- NIST SP 800-53A::SC-18 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-18 (1)
- NIST SP 800-53 Revision 5::SC-18 (1)

1.135 O365-WD-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

In Word, macros must be blocked from running, even if Enable all macros is selected in the Macro Settings section of the Trust Center.

```
GROUP ID: V-223415
RULE ID: SV-223415r961092
```

Rationale:

This policy setting allows you to block macros from running in Office files that come from the Internet. If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to "Enable Content", users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

If you disable or do not configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center "Block macros from running in Office files from the Internet" is set to "Enabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\16.0\word\security

If the value blockcontentexecutionfrominternet is REG_DWORD = 1, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center "Block macros from running in Office files from the Internet" to "Enabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.136 O365-WD-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Trusted Locations on the network must be disabled in Word.

```
GROUP ID: V-223416
RULE ID: SV-223416r961092
```

Rationale:

This policy setting controls whether trusted locations on the network can be used.

If you enable this policy setting, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by clicking the "Add new location" button in the Trusted Locations section of the Trust Center. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

If you disable this policy setting, the selected application ignores any network locations listed in the Trusted Locations section of the Trust Center.

If you also deploy Trusted Locations via Group Policy, you should verify whether any of them are remote locations. If any of them are remote locations and you do not allow remote locations via this policy setting, those policy keys that point to remote locations will be ignored on client computers.

Disabling this policy setting does not delete any network locations from the Trusted Locations list, but causes disruption for users who add network locations to the Trusted Locations list. Users are also prevented from adding new network locations to the Trusted Locations list in the Trust Center. We recommended that you do not enable this policy setting as the "Allow Trusted Locations on my network (not recommended)" check box also states. Therefore, in practice, it should be possible to disable this policy setting in most situations without causing significant usability issues for most users.

If you do not enable this policy setting, users can select the "Allow Trusted Locations on my network (not recommended)" check box if desired and then specify trusted locations by clicking the "Add new location" button.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Trusted Locations >> Allow Trusted Locations on the network is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\word\security\trusted locations

If the value for allownetworklocations is REG_DWORD = 0, this is not a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Trust Center >> Trusted Locations >> Allow Trusted Locations on the network to "Disabled".

Additional Information:

CCI-001170 Prevents the automatic execution of mobile code in organization-defined software applications.

- NIST SP 800-53::SC-18 (4)
- NIST SP 800-53A::SC-18 (4).1 (iii) (iv)
- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.137 O365-WD-000018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

VBA Macros not digitally signed must be blocked in Word.

```
GROUP ID: V-223417
RULE ID: SV-223417r960963
```

Rationale:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If you enable this policy setting, you can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office. This option also allows users to potentially enable unsigned/untrusted macros. If a site requires the use of macros, they must be signed /approved and added to appropriate locations listed in the Trust Center Settings.
- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.
- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.
- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Security >> Trust Center >> "VBA macro Notification Settings" is set to "Enabled" and "Disable all except digitally signed macros" from the Options.

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\Microsoft\office\16.0\word\security

If the value vbawarnings is REG_DWORD = 3, this is not a finding. A value of REG_DWORD = 4 is also acceptable. If the registry key does not exist or is not configured properly, this is a finding.

Remediation:

Set the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Security >> Trust Center >> "VBA macro Notification Settings" to "Enabled" and "Disable all except digitally signed macros" from the Options.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.138 O365-WD-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

File validation in Word must be enabled.

```
GROUP ID: V-223418
RULE ID: SV-223418r960921
```

Rationale:

This policy setting allows the file validation feature to be turned off.

If this policy setting is enabled, file validation will be turned off.

If this policy setting is disabled or not configured, file validation will be turned on. Office Binary Documents (97-2003) are checked to see if they conform to the file format schema before they are opened.

Audit:

Verify the policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Turn off file validation is set to "Disabled".

Use the Windows Registry Editor to navigate to the following key:

HKCU\software\policies\microsoft\office\16.0\word\security\filevalidation

If the value for enableonload is REG_DWORD = 1, this is not a finding.

Remediation:

Set policy value for User Configuration >> Administrative Templates >> Microsoft Word 2016 >> Word Options >> Security >> Turn off file validation to "Disabled".

Additional Information:

CCI-001695 Prevent the execution of organization-defined unacceptable mobile code.

- NIST SP 800-53::SC-18 (3)
- NIST SP 800-53 Revision 4::SC-18 (3)
- NIST SP 800-53 Revision 5::SC-18 (3)
- NIST SP 800-53A::SC-18 (3).1

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	O365-AC-000001 (Manual)	☐	☐
1.2	O365-AC-000002 (Manual)	☐	☐
1.3	O365-AC-000003 (Manual)	☐	☐
1.4	O365-CO-000001 (Manual)	☐	☐
1.5	O365-CO-000002 (Manual)	☐	☐
1.6	O365-CO-000003 (Manual)	☐	☐
1.7	O365-CO-000004 (Manual)	☐	☐
1.8	O365-CO-000005 (Manual)	☐	☐
1.9	O365-CO-000006 (Manual)	☐	☐
1.10	O365-CO-000007 (Manual)	☐	☐
1.11	O365-CO-000008 (Manual)	☐	☐
1.12	O365-CO-000009 (Manual)	☐	☐
1.13	O365-CO-000010 (Manual)	☐	☐
1.14	O365-CO-000012 (Manual)	☐	☐
1.15	O365-CO-000013 (Manual)	☐	☐
1.16	O365-CO-000014 (Manual)	☐	☐
1.17	O365-CO-000015 (Manual)	☐	☐
1.18	O365-CO-000016 (Manual)	☐	☐
1.19	O365-CO-000017 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	O365-CO-000018 (Manual)	☐	☐
1.21	O365-CO-000019 (Manual)	☐	☐
1.22	O365-CO-000021 (Manual)	☐	☐
1.23	O365-CO-000020 (Manual)	☐	☐
1.24	O365-CO-000022 (Manual)	☐	☐
1.25	O365-CO-000023 (Manual)	☐	☐
1.26	O365-CO-000024 (Manual)	☐	☐
1.27	O365-CO-000025 (Manual)	☐	☐
1.28	O365-CO-000026 (Manual)	☐	☐
1.29	O365-CO-000027 (Manual)	☐	☐
1.30	O365-EX-000001 (Manual)	☐	☐
1.31	O365-EX-000002 (Manual)	☐	☐
1.32	O365-EX-000003 (Manual)	☐	☐
1.33	O365-EX-000004 (Manual)	☐	☐
1.34	O365-EX-000005 (Manual)	☐	☐
1.35	O365-EX-000007 (Manual)	☐	☐
1.36	O365-EX-000006 (Manual)	☐	☐
1.37	O365-EX-000008 (Manual)	☐	☐
1.38	O365-EX-000009 (Manual)	☐	☐
1.39	O365-EX-000010 (Manual)	☐	☐
1.40	O365-EX-000011 (Manual)	☐	☐
1.41	O365-EX-000012 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	O365-EX-000013 (Manual)	☐	☐
1.43	O365-EX-000014 (Manual)	☐	☐
1.44	O365-EX-000015 (Manual)	☐	☐
1.45	O365-EX-000016 (Manual)	☐	☐
1.46	O365-EX-000017 (Manual)	☐	☐
1.47	O365-EX-000018 (Manual)	☐	☐
1.48	O365-EX-000019 (Manual)	☐	☐
1.49	O365-EX-000020 (Manual)	☐	☐
1.50	O365-EX-000021 (Manual)	☐	☐
1.51	O365-EX-000022 (Manual)	☐	☐
1.52	O365-EX-000023 (Manual)	☐	☐
1.53	O365-EX-000024 (Manual)	☐	☐
1.54	O365-EX-000025 (Manual)	☐	☐
1.55	O365-EX-000026 (Manual)	☐	☐
1.56	O365-EX-000027 (Manual)	☐	☐
1.57	O365-EX-000028 (Manual)	☐	☐
1.58	O365-EX-000029 (Manual)	☐	☐
1.59	O365-EX-000030 (Manual)	☐	☐
1.60	O365-EX-000031 (Manual)	☐	☐
1.61	O365-EX-000032 (Manual)	☐	☐
1.62	O365-EX-000033 (Manual)	☐	☐
1.63	O365-EX-000034 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	O365-LY-000001 (Manual)	☐	☐
1.65	O365-LY-000002 (Manual)	☐	☐
1.66	O365-OU-000001 (Manual)	☐	☐
1.67	O365-OU-000002 (Manual)	☐	☐
1.68	O365-OU-000003 (Manual)	☐	☐
1.69	O365-OU-000004 (Manual)	☐	☐
1.70	O365-OU-000005 (Manual)	☐	☐
1.71	O365-OU-000006 (Manual)	☐	☐
1.72	O365-OU-000007 (Manual)	☐	☐
1.73	O365-OU-000008 (Manual)	☐	☐
1.74	O365-OU-000009 (Manual)	☐	☐
1.75	O365-OU-000010 (Manual)	☐	☐
1.76	O365-OU-000011 (Manual)	☐	☐
1.77	O365-OU-000012 (Manual)	☐	☐
1.78	O365-OU-000013 (Manual)	☐	☐
1.79	O365-OU-000014 (Manual)	☐	☐
1.80	O365-OU-000015 (Manual)	☐	☐
1.81	O365-OU-000016 (Manual)	☐	☐
1.82	O365-OU-000017 (Manual)	☐	☐
1.83	O365-OU-000018 (Manual)	☐	☐
1.84	O365-OU-000019 (Manual)	☐	☐
1.85	O365-OU-000020 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	O365-OU-000021 (Manual)	☐	☐
1.87	O365-OU-000022 (Manual)	☐	☐
1.88	O365-OU-000023 (Manual)	☐	☐
1.89	O365-OU-000024 (Manual)	☐	☐
1.90	O365-OU-000025 (Manual)	☐	☐
1.91	O365-OU-000026 (Manual)	☐	☐
1.92	O365-OU-000027 (Manual)	☐	☐
1.93	O365-OU-000028 (Manual)	☐	☐
1.94	O365-PR-000001 (Manual)	☐	☐
1.95	O365-PR-000002 (Manual)	☐	☐
1.96	O365-PR-000003 (Manual)	☐	☐
1.97	O365-PT-000001 (Manual)	☐	☐
1.98	O365-PT-000002 (Manual)	☐	☐
1.99	O365-PT-000003 (Manual)	☐	☐
1.100	O365-PT-000004 (Manual)	☐	☐
1.101	O365-PT-000005 (Manual)	☐	☐
1.102	O365-PT-000006 (Manual)	☐	☐
1.103	O365-PT-000007 (Manual)	☐	☐
1.104	O365-PT-000008 (Manual)	☐	☐
1.105	O365-PT-000009 (Manual)	☐	☐
1.106	O365-PT-000010 (Manual)	☐	☐
1.107	O365-PT-000011 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	O365-PT-000012 (Manual)	☐	☐
1.109	O365-PT-000013 (Manual)	☐	☐
1.110	O365-PU-000001 (Manual)	☐	☐
1.111	O365-PU-000002 (Manual)	☐	☐
1.112	O365-PU-000003 (Manual)	☐	☐
1.113	O365-VI-000001 (Manual)	☐	☐
1.114	O365-VI-000002 (Manual)	☐	☐
1.115	O365-VI-000003 (Manual)	☐	☐
1.116	O365-VI-000004 (Manual)	☐	☐
1.117	O365-VI-000005 (Manual)	☐	☐
1.118	O365-VI-000006 (Manual)	☐	☐
1.119	O365-VI-000007 (Manual)	☐	☐
1.120	O365-WD-000001 (Manual)	☐	☐
1.121	O365-WD-000002 (Manual)	☐	☐
1.122	O365-WD-000003 (Manual)	☐	☐
1.123	O365-WD-000004 (Manual)	☐	☐
1.124	O365-WD-000005 (Manual)	☐	☐
1.125	O365-WD-000006 (Manual)	☐	☐
1.126	O365-WD-000007 (Manual)	☐	☐
1.127	O365-WD-000008 (Manual)	☐	☐
1.128	O365-WD-000009 (Manual)	☐	☐
1.129	O365-WD-000010 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	O365-WD-000011 (Manual)	☐	☐
1.131	O365-WD-000012 (Manual)	☐	☐
1.132	O365-WD-000013 (Manual)	☐	☐
1.133	O365-WD-000014 (Manual)	☐	☐
1.134	O365-WD-000015 (Manual)	☐	☐
1.135	O365-WD-000016 (Manual)	☐	☐
1.136	O365-WD-000017 (Manual)	☐	☐
1.137	O365-WD-000018 (Manual)	☐	☐
1.138	O365-WD-000019 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
9/11/2025	V1.0.0	Initial CIS Release