CIS Microsoft Exchange 2019 Mailbox Server STIG Benchmark

v1.0.0 - 08-14-2025

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 Exchange 2019 Mailbox Server Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 24 Oct 2024

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 Exchange 2019 Mailbox Server 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 Exchange 2019 Mailbox Server

Recommendations

1 STIG RULES

Microsoft Exchange Server 2019

Microsoft Exchange 2019 Mailbox Server Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 24 Oct 2024

CLASSIFICATION unclassified

1.1 EX19-MB-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must use encryption for RPC client access.

```
GROUP ID: V-259645
RULE ID: SV-259645r960759
```

Rationale:

This setting controls whether client machines are forced to use secure channels to communicate with the server. If this feature is enabled, clients will only be able to communicate with the serv

er over secure communication channels.

Failure to require secure connections to the client access server increases the potential for unintended eavesdropping or data loss.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-RpcClientAccess | Select-Object -Property Server, Name,
EncryptionRequired
```

If the value of "EncryptionRequired" is not set to "True", this is a finding.

Note: This is configured as "True" by default.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-RpcClientAccess -Server <ServerName> -EncryptionRequired $true
```

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.2 EX19-MB-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must use encryption for Outlook Web App (OWA) access.

```
GROUP ID: V-259646
RULE ID: SV-259646r960759
```

Rationale:

This setting controls whether client machines should be forced to use secure channels to communicate with this virtual directory. If this feature is enabled, clients will only be able to communicate with the directory if they are capable of supporting secure communication with the server.

The use of secure communication prevents eavesdroppers from reading or modifying communications between servers and clients. The network and DMZ STIG identify criteria for OWA and Public Folder configuration in the network, including Common Access Card (CAC)-enabled preauthentication through an application firewall proxy.

Failure to require secure connections on a website increases the potential for unintended eavesdropping or data loss.

Audit:

Open an Exchange Management Shell and enter the following command:

```
Get-ExchangeCertificate |Select-Object -Property Subject,Services,Thumbprint
```

If the certificate associated with the IIS service is not a trusted public certificate, this is a finding.

In the same Exchange Management Shell, run the following cmdlets:

```
Get-OwaVirtualDirectory | Select-Object -Property internalurl, externalurl
```

If the value returned is not https://, this is a finding.

Open IIS Manager and locate the Exchange Server. In the navigation pane on the left, navigate to Sites >> Default Web Site >> owa. In the pane on the right, under /owa Home, in the IIS section, double-click "SSL Settings".

If the box "Require SSL" is not checked, this is a finding.

Remediation:

Ensure a trusted public certificate is installed for the Exchange server with the correct FQDNs that will service the domain. This will allow secure communications between clients and the server. This should be done before the server is put into production.

Once installed, in an elevated Exchange Management Shell, run the following cmdlet to associate the certificate with the IIS service:

Enable-ExchangeCertificate -Thumbprint -Services IIS

Set the OWA URL to use HTTPS instead of HTTP by updating the URLs to HTTPS.

If the website is "http://mail.contoso.com" for both internal and external (for example), run the following cmdlet to set it to HTTPS:

```
Set-OwaVirtualDirectory -Identity "<Server>\owa (Default Web Site) -
InternalUrl "https://mail.contoso.com/owa" -ExternalUrl
"https://mail.contoso.com/owa"
```

Note: If this change is made, it must be done for the ECP virtual directory as well. A warning notifies users that this must be done.

Open IIS Manager and locate the Exchange Server. In the navigation pane on the left, navigate to Sites >> Default Web Site >> owa. In the pane on the right, under /owa Home, in the IIS section, double-click "SSL Settings".

Check the box for "Require SSL".

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.3 EX19-MB-000008 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have forms-based authentication enabled.

```
GROUP ID: V-259647
RULE ID: SV-259647r960759
```

Rationale:

Identification and Authentication provide the foundation for access control. Access to email services applications in the DOD requires authentication using DOD Public Key Infrastructure (PKI) certificates. Authentication for Outlook Web App (OWA) is used to enable web access to user email mailboxes and should assume that certificate-based authentication has been configured. This setting controls whether forms-based logon should be used by the OWA website.

Because the DOD requires Common Access Card (CAC)-based authentication to applications, OWA access must be brokered through an application proxy or other preauthenticator, which performs CAC authentication prior to arrival at the CA server. The authenticated request is then forwarded directly to OWA, where authentication is repeated without requiring the user to repeat authentication steps. For this scenario to work, the Application Proxy server must have forms-based authentication enabled, and Exchange must have forms-based Authentication disabled.

If forms-based Authentication is enabled on the Exchange CA server, it is evidence that the application proxy server is either not correctly configured, or it may be missing.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-OwaVirtualDirectory | Select-Object -Property ServerName, Name, Identity,
*Authentication
```

If the value of "FormsAuthentication" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-OwaVirtualDirectory -Identity <'IdentityName'> -FormsAuthentication
$false
```

Note: <IdentityName> must be in quotes.

Example for the Identity Name: <ServerName>\owa (Default website)

Restart the IIS service.

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.4 EX19-MB-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have administrator audit logging enabled.

```
GROUP ID: V-259648
RULE ID: SV-259648r960780
```

Rationale:

Unauthorized or malicious data changes can compromise the integrity and usefulness of the data. Automated attacks or malicious users with elevated privileges have the ability to effect change using the same mechanisms as email administrators. Auditing any changes to access mechanisms not only supports accountability and nonrepudiation for those authorized to define the environment but also enables investigation of changes made by others who may not be authorized.

Note: This administrator auditing feature audits all exchange changes regardless of the user's assigned role or permissions.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-AdminAuditLogConfig | Select-Object -Property  Name, AdminAuditLogEnabled
```

If the value of "AdminAuditLogEnabled" is not set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true
```

Additional Information:

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

1.5 EX19-MB-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange servers must use approved DOD certificates.

```
GROUP ID: V-259649
RULE ID: SV-259649r960792
```

Rationale:

Server certificates are required for many security features in Exchange; without them, the server cannot engage in many forms of secure communication.

Failure to implement valid certificates makes it virtually impossible to secure Exchange's communications.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-ExchangeCertificate | Select-Object -Property CertificateDomains, issuer
```

If the value of "CertificateDomains" does not indicate it is issued by the DOD, this is a finding.

Remediation:

Remove the non-DOD certificate and import the correct DOD certificates.

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.6 EX19-MB-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have authenticated access set to integrated Windows authentication only.

```
GROUP ID: V-259650
RULE ID: SV-259650r960792
```

Rationale:

To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DOD-approved PKIs, all DOD systems (e.g., networks, web servers, and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

This requirement is applicable to access control enforcement applications (e.g., authentication servers) and other applications that perform information and system access control functions.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-OwaVirtualDirectory | Select-Object -Property ServerName, Name,
Identity,*Authentication
```

If the value of "WindowsAuthentication" is not set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-OwaVirtualDirectory -Identity '<IdentityName>' -WindowsAuthentication
$true
```

Note: The <IdentityName> value must be in quotes.

Example for the Identity Name: <ServerName>\owa (Default website)

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

1.7 EX19-MB-000021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange auto-forwarding email to remote domains must be disabled or restricted.

```
GROUP ID: V-259651
RULE ID: SV-259651r960801
```

Rationale:

Attackers can use automated messages to determine whether a user account is active, in the office, traveling, and so on. An attacker might use this information to conduct future attacks. Verify Automatic Forwards to remote domains are disabled, except for enterprise mail that must be restricted to forward only to .mil and .gov. domains.

Before enabling this setting, configure a remote domain.

Audit:

Note: This requirement is not applicable on classified or completely closed networks.

For Non-Enterprise Mail:

Open the Exchange Management Shell and enter the following command:

```
Get-RemoteDomain | Select-Object -Property Identity, AutoForwardEnabled
```

If the value of AutoForwardEnabled is not set to "False", this is a finding.

For Enterprise Mail:

If the value of "AutoForwardEnabled" is set to "True", this is not a finding.

and

In the Exchange Management Shell, enter the following command:

Get-RemoteDomain

If the value of "RemoteDomain" is not set to ".mil" and/or ".gov" domain(s), this is a finding.

Remediation:

For Non-Enterprise Mail:

Open the Exchange Management Shell and enter the following command:

```
Set-RemoteDomain -Identity <'IdentityName'> -AutoForwardEnabled $false
```

Note: The <IdentityName> value must be in quotes.

For Enterprise Mail:

```
New-RemoteDomain -Name <NewRemoteDomainName> -DomainName <SMTP Address>
```

Note: <NewRemoteDomainName> must either be a .mil or .gov domain.

```
Set-RemoteDomain -Identity <'RemoteDomainIdentity'> -AutoForwardEnabled $true
```

Note: The <RemoteDomainIdentity> value must be in quotes.

Additional Information:

CCI-001368 Enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.8 EX19-MB-000031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange connectivity logging must be enabled.

```
GROUP ID: V-259652
RULE ID: SV-259652r960879
```

Rationale:

A connectivity log is a record of the SMTP connection activity of the outbound message delivery queues to the destination Mailbox server, smart host, or domain. Connectivity logging is available on Mailbox servers in Exchange 2019 as it holds Mailbox, Client Access, and Hub Transport roles. This must also be completed on Edge Transport servers, as that is a separate role. By default, connectivity logging is disabled. If events are not recorded, it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Note: Transport configuration settings apply to the organization/global level of the Exchange SMTP path. By checking and setting them on the Mailbox server, the setting will apply to both Hub and Edge server roles.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-TransportService | Select-Object -Property Name, Identity,
ConnectivityLogEnabled
```

If the value of "ConnectivityLogEnabled" is not set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-TransportService -Identity <'IdentityName'> -ConnectivityLogEnabled $true
```

Note: The <IdentityName> value must be in quotes.

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

1.9 EX19-MB-000032 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange email diagnostic log level must be set to the lowest level.

```
GROUP ID: V-259653
RULE ID: SV-259653r960879
```

Rationale:

Log files help establish a history of activities and can be useful in detecting attack attempts or determining tuning adjustments to improve availability. Diagnostic logging, however, characteristically produces large volumes of data and requires care in managing the logs to prevent risk of disk capacity denial-of-service conditions.

Exchange diagnostic logging is divided into 29 main "services", each of which has anywhere from two to 26 "categories" of events to be monitored. Each category may be set to one of four levels of logging: Lowest, Low, Medium, and High, depending on how much detail is required. Higher levels of detail require more disk space to store the audit material.

Diagnostic logging is intended to help administrators debug problems with their systems, not as a general-purpose auditing tool. Because the diagnostic logs collect a great amount of information, the log files may grow large very quickly. Diagnostic log levels may be raised for limited periods of time when attempting to debug relevant pieces of Exchange functionality. Once debugging has finished, diagnostic log levels should be reduced again.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-EventLogLevel
```

If the Diagnostic of any EventLevel is not set to "Lowest", this is a finding.

Note: Default installation of Exchange has all Event Levels set to Lowest with exception of the following:

- MSExchange ADAccess\Topology - Low
- MSExchangeADAccess\Validation - Low
- MSExchange BackEndRehydration\Configuration - Low
- MSExchange BackEndRehydration\Server - 2
- MSExchange OAuth\Configuration - Low
- MSExchange OAuth\Server - 2
- MSExchange RBAC\RBAC - Low
- MSExchangeADTopology\Topology - Low

All of these must be set to "Lowest".

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-EventLogLevel -Identity <'IdentityName\EventlogName'> -Level Lowest
```

Note: The <IdentityName\EventlogName> value must be in quotes.

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

1.10 EX19-MB-000033 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange audit record parameters must be set.

```
GROUP ID: V-259654
RULE ID: SV-259654r960879
```

Rationale:

Log files help establish a history of activities and can be useful in detecting attack attempts. This item declares the fields that must be available in the audit log file to adequately research events that are logged.

Audit records should include the following fields to supply useful event accounting: Object modified, Cmdlet name, Cmdlet parameters, Modified parameters, Caller, Succeeded, and Originating server.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-AdminAuditLogConfig | Select-Object -Property AdminAuditLogParameters
```

Note: The value of "*" indicates all parameters are being audited.

If the value of "AdminAuditLogParameters" is not set to "*", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-AdminAuditLogConfig -AdminAuditLogParameters *
```

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

1.11 EX19-MB-000034 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The RBAC role for audit log management must be defined and restricted.

```
GROUP ID: V-259655
RULE ID: SV-259655r960882
```

Rationale:

The RBAC role for the audit log management "Audit Log Role" should be defined in the Organizational or Enterprise Domain Security Plan (EDSP) to define the necessary personnel that are required to handle audit logs for the Microsoft Exchange application.

Group membership should be audited regularly by checking the EDSP regularly and determine who should and should not have group membership.

There are three built-in groups that automatically have membership: Organization Management, Compliance Management, and Records Management.

Audit:

Refer to the EDSP on who should be in the RBAC role group "Audit Log". It is automatically assigned to those in the Organization Management role group.

In an Exchange management shell, run the following cmdlet:

```
Get-RoleGroup "Records Management"|Get-RoleGroupMember
```

Unless specified in the EDSP that custom role group is specified for this permission, if this role group is empty this is a finding.

Remediation:

Refer to the EDSP on who should have the RBAC role "Audit Log". If a custom RBAC role is designated for the Audit Log role, ensure that the custom RBAC role group is populated.

Follow the rule of least privilege.

Otherwise, in an Exchange management shell, run the following:

```
"Add-RoleGroupMember -Identity "Records Management" -Member <user>"
```

Where is the personnel responsible for handling audit logs.

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

1.12 EX19-MB-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange email subject line logging must be disabled.

```
GROUP ID: V-259656
RULE ID: SV-259656r960900
```

Rationale:

Log files help establish a history of activities and can be useful in detecting attack attempts or determining tuning adjustments to improve availability. When "message tracking" is enabled, only the sender, recipients, time, and other delivery information is included by default. Information such as the subject and message body is not included.

However, the absence of the message subject line can make it difficult to locate a specific message in the log unless one knows roughly what time the message was sent. To simplify searches through these logs, Exchange offers the ability to include the message "subject line" in the log files and in the Message Tracking Center display. This can make it significantly easier to locate a specific message.

However, this feature creates larger log files and will contain information that may raise privacy and legal concerns. Enterprise policy should be consulted before this feature is enabled. Also, because the log files may contain sensitive information in the form of the subject line, the log files will need to be protected, commensurate with the sensitivity level, as the content may be of interest to an attacker.

For these reasons, it is recommended that subject logging not be enabled during regular production operations. Instead, treat this feature as a diagnostic that can be used if needed. The tradeoff is that finding the correct message in the message tracking logs will become more difficult because the administrator will need to search using only the time the message was sent and the message's sender. This control will have no effect unless Message Tracking is enabled. However, the setting should be disabled in case message tracking is enabled in the future.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-TransportService | Select-Object -Property Name, Identity,
MessageTrackingLogSubjectLoggingEnabled
```

If the value of "MessageTrackingLogSubjectLoggingEnabled" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-Transportservice -MessageTrackingLogSubjectLoggingEnabled $False
```

Additional Information:

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

1.13 EX19-MB-000041 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange message tracking logging must be enabled.

```
GROUP ID: V-259657
RULE ID: SV-259657r960900
```

Rationale:

A message tracking log provides a detailed log of all message activity as messages are transferred to and from a computer running Exchange.

If events are not recorded, it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-TransportService | Select-Object -Property Name,
MessageTrackingLogEnabled
```

If the value of MessageTrackingLogEnabled is not set to True, this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-TransportService <IdentityName> -MessageTrackingLogEnabled $true
```

Note: The <IdentityName> value must be in quotes.

Additional Information:

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

1.14 EX19-MB-000042 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange circular logging must be disabled.

```
GROUP ID: V-259658
RULE ID: SV-259658r960900
```

Rationale:

Logging provides a history of events performed and can also provide evidence of tampering or attack. Failure to create and preserve logs adds to the risk that suspicious events may go unnoticed and raises the potential that insufficient history will be available to investigate them.

This setting controls how log files are written. If circular logging is enabled, one log file is stored with a default size of 1024 KB. Once the size limit has been reached, additional log entries overwrite the oldest log entries. If circular logging is disabled, once a log file reaches the size limit, a new log file is created.

Mailbox should not use circular logging. Logs should be written to a partition separate from the operating system, with log protection and backups being incorporated into the overall System Security Plan.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-MailboxDatabase | Select-Object -Property Name, Identity,
CircularLoggingEnabled
```

If the value of "CircularLoggingEnabled" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-MailboxDatabase -Identity <'IdentityName'> -CircularLoggingEnabled $false
```

Note: The <IdentityName> value must be in quotes.

Additional Information:

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

1.15 EX19-MB-000048 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange queue monitoring must be configured with threshold and action.

```
GROUP ID: V-259659
RULE ID: SV-259659r960918
```

Rationale:

Monitors are automated "process watchers" that respond to performance changes and can be useful in detecting outages and alerting administrators where attention is needed. Exchange has built-in monitors that enable the administrator to generate alerts if thresholds are reached, better enabling them to react in a timely fashion.

This field offers choices of alerts when a "warning" or "critical" threshold is reached on the SMTP queue. A good rule of thumb (default) is to issue warnings when SMTP queue growth exceeds 10 minutes and critical messages when it exceeds 20 minutes, which should only happen occasionally. Frequent alerts against this counter may indicate a network or other issue (such as inbound ExchangeMER traffic) that directly impacts email delivery.

Notification choices include email alert to an email-enabled account (for example, an email administrator) or invoke a script to take other action (for example, to add an event to the Microsoft Application Event Log, where external monitors might detect it).

Audit:

Note: If a third-party application is performing monitoring functions, the reviewer should verify the application is monitoring correctly and mark the vulnerability not applicable (NA).

Open the Exchange Management Shell and enter the following command:

```
perfmon
Get-MonitoringItemHelp -Identity <String> -Server <ServerIdParameter>
```

If no sets are defined or queues are not being monitored, this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
perfmon
```

In the left pane, navigate to and select Performance >> Data Collector Sets >> User Defined.

Right-click and navigate to User Defined >> New >> Data Collector Sets and configure the system to use the data collection set for monitoring the queues.

Additional Information:

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53::AU-6 (4)
- NIST SP 800-53A::AU-6 (4).1
- NIST SP 800-53 Revision 4::AU-6 (4)
- NIST SP 800-53 Revision 5::AU-6 (4)

1.16 EX19-MB-000052 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must protect audit data against unauthorized read access.

```
GROUP ID: V-259660
RULE ID: SV-259660r960930
```

Rationale:

Log files help establish a history of activities and can be useful in detecting attack attempts or determining tuning adjustments to improve availability. Audit log content must always be considered sensitive and in need of protection. Audit data available for modification by a malicious user can be altered to conceal malicious activity. Audit data might also provide a means for the malicious user to plan unauthorized activities that exploit weaknesses.

The contents of audit logs are protected against unauthorized access, modification, or deletion. Only authorized auditors and the audit functions should be granted "Read" and "Write" access to audit log data.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the authorized groups or users that should have "Read" access to the audit data.

By default, the logs are located on the application partition in \Program Files\Microsoft\Exchange Server\V15\Logging.

If any group or user has "Read" access to the audit data that is not documented in the EDSP, this is a finding.

Remediation:

Update the EDSP to specify the authorized groups or users that should have "Read" access to the audit data or verify that this information is documented by the organization.

Restrict any unauthorized groups' or users' "Read" access to the audit logs.

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

1.17 EX19-MB-000053 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must protect audit data against unauthorized access.

```
GROUP ID: V-259661
RULE ID: SV-259661r960933
```

Rationale:

Log files help establish a history of activities and can be useful in detecting attack attempts or determining tuning adjustments to improve availability. Audit log content must always be considered sensitive and in need of protection. Audit data available for modification by a malicious user can be altered to conceal malicious activity. Audit data might also provide a means for the malicious user to plan unauthorized activities that exploit weaknesses.

The contents of audit logs are protected against unauthorized access, modification, or deletion. Only authorized auditors and the audit functions should be granted "Read" and "Write" access to audit log data.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the authorized groups or users that should have access to the audit data.

By default, the logs are located on the application partition in \Program Files\Microsoft\Exchange Server\V15\Logging.

If any group or user has modify privileges for the audit data that is not documented in the EDSP, this is a finding.

Remediation:

Update the EDSP to specify the authorized groups or users that should have access to the audit data or verify that this information is documented by the organization.

Restrict any unauthorized groups' or users' modify permissions for the audit logs.

Additional Information:

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

1.18 EX19-MB-000054 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must protect audit data against unauthorized deletion.

```
GROUP ID: V-259662
RULE ID: SV-259662r960936
```

Rationale:

Log files help establish a history of activities and can be useful in detecting attack attempts or determining tuning adjustments to improve availability. Audit log content must always be considered sensitive and in need of protection. Audit data available for modification by a malicious user can be altered to conceal malicious activity. Audit data might also provide a means for the malicious user to plan unauthorized activities that exploit weaknesses.

The contents of audit logs are protected against unauthorized access, modification, or deletion. Only authorized auditors and the audit functions should be granted "Read" and "Write" access to audit log data.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the authorized groups or users that should have "Delete" permissions for the audit data.

By default, the logs are located on the application partition in \Program Files\Microsoft\Exchange Server\V15\Logging.

If any group or user has "Delete" permissions for the audit data that is not documented in the EDSP, this is a finding.

Remediation:

Update the EDSP to specify the authorized groups or users that should have "Delete" permissions for the audit data or verify that this information is documented by the organization.

Restrict any unauthorized groups' or users' "Delete" permissions for the audit logs.

Additional Information:

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

1.19 EX19-MB-000058 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange audit data must be on separate partitions.

```
GROUP ID: V-259663
RULE ID: SV-259663r960948
```

Rationale:

Log files help establish a history of activities and can be useful in detecting attack attempts or determining tuning adjustments to improve availability. Audit log content must always be considered sensitive and in need of protection.

Successful exploit of an application server vulnerability may well be logged by monitoring or audit processes when it occurs. Writing log and audit data to a separate partition where separate security contexts protect them may offer the ability to protect this information from being modified or removed by the exploit mechanism.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the audit logs' assigned partition.

By default, the logs are located on the application partition in \Program Files\Microsoft\Exchange Server\V15\Logging.

If the log files are not on a separate partition from the application, this is a finding.

Remediation:

Update the EDSP to specify the audit logs' assigned partition or verify that this information is documented by the organization.

Configure the audit log location to be on a partition drive separate from the application.

Additional Information:

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

1.20 EX19-MB-000061 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange local machine policy must require signed scripts.

```
GROUP ID: V-259664
RULE ID: SV-259664r1015275
```

Rationale:

Scripts often provide a way for attackers to infiltrate a system, especially scripts downloaded from untrusted locations. By setting machine policy to prevent unauthorized script executions, unanticipated system impacts can be avoided. Failure to allow only signed remote scripts reduces the attack vector vulnerabilities from unsigned remote scripts.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-ExecutionPolicy
```

If the value returned is not "RemoteSigned", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ExecutionPolicy RemoteSigned
```

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)

1.21 EX19-MB-000063 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Send Fatal Errors to Microsoft must be disabled.

```
GROUP ID: V-259665
RULE ID: SV-259665r960963
```

Rationale:

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of nonessential capabilities include but are not limited to advertising software or browser plug-ins not related to requirements or providing a wide array of functionality not required for every mission but that cannot be disabled.

All system errors in Exchange will result in outbound traffic that may be identified by an eavesdropper. For this reason, the "Report Fatal Errors to Microsoft" feature must be disabled.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-ExchangeServer -status | Select-Object -Property Name, Identity,
ErrorReportingEnabled
```

For each Exchange Server, if the value of "ErrorReportingEnabled" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ExchangeServer -Identity <'IdentityName'> -ErrorReportingEnabled $false
```

Note: The <IdentityName> value must be in quotes.

Repeat the process for each Exchange Server.

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

1.22 EX19-MB-000064 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must not send customer experience reports to Microsoft.

```
GROUP ID: V-259666
RULE ID: SV-259666r960963
```

Rationale:

It is detrimental for applications to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of nonessential capabilities include, but are not limited to, advertising software or browser plug-ins not related to requirements or providing a wide array of functionality not required for every mission but that cannot be disabled.

Customer Experience reports in Exchange will result in outbound traffic that may be identified by an eavesdropper. For this reason, the Customer Experience reports must not be sent to Microsoft.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-OrganizationConfig | Select-Object -Property CustomerFeedbackEnabled
```

If the value for "CustomerFeedbackEnabled" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-OrganizationConfig -CustomerFeedbackEnabled $false
```

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

1.23 EX19-MB-000065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Internet Message Access Protocol 4 (IMAP4) service must be disabled.

```
GROUP ID: V-259667
RULE ID: SV-259667r960963
```

Rationale:

IMAP4 is not approved for use within the DOD. It uses a clear-text-based user name and password and does not support the DOD standard for PKI for email access. User name and password could easily be captured from the network, allowing a malicious user to access other system features. Uninstalling or disabling the service will prevent the use of the IMAP4 protocol.

Audit:

Note: This requirement applies to IMAP4. IMAP Secure is not restricted and does not apply to this requirement.

Open the Windows PowerShell and enter the following command:

```
Get-Service -Name MSExchangeIMAPBE,MSExchangeImap4 |Select-Object -Property
Name,StartType
```

If ANY of the IMAP services StartType is NOT set to "Disabled", this is a finding.

Remediation:

Open the Windows PowerShell in an Elevated Prompt and enter the following commands:

```
Get-Service -Name MSExchangeIMAPBE,MSExchangeImap4 |ForEach-Object {Set-
Service -Name $_.Name -StartupType Disabled}
```

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

1.24 EX19-MB-000066 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Post Office Protocol 3 (POP3) service must be disabled.

```
GROUP ID: V-259668
RULE ID: SV-259668r960963
```

Rationale:

POP3 is not approved for use within the DOD. It uses a clear-text-based user name and password and does not support the DOD standard for PKI for email access. User name and password could easily be captured from the network, allowing a malicious user to access other system features. Uninstalling or disabling the service will prevent the use of POP3.

Audit:

```
Get-Service -Name MSExchangePop3,MSExchangePOP3BE |Select-Object -Property
Name,StartType
```

If any of the POP3 services StartType is NOT set to "Disabled", this is a finding.

Remediation:

Open the Windows PowerShell in an Elevated Prompt and enter the following commands:

```
Get-Service -Name MSExchangePop3,MSExchangePOP3BE |ForEach-Object {Set-
Service -Name $_.Name -StartupType Disabled}
```

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

1.25 EX19-MB-000105 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Mailbox databases must reside on a dedicated partition.

```
GROUP ID: V-259669
RULE ID: SV-259669r961095
```

Rationale:

In the same way that added security layers can provide a cumulative positive effect on security posture, multiple applications can provide a cumulative negative effect. A vulnerability and subsequent exploit to one application can lead to an exploit of other applications sharing the same security context. For example, an exploit to a web server process that leads to unauthorized administrative access to the host system can most likely lead to a compromise of all applications hosted by the same system.

Email services should be installed to a discrete set of directories on a partition that does not host other applications. Email services should never be installed on a Domain Controller/Directory Services server.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the location where the Exchange Mailbox databases reside.

Open the Exchange Management Shell and enter the following command:

```
Get-MailboxDatabase | Select-Object -Property Name, Identity, EdbFilePath
```

Open Windows Explorer, navigate to the mailbox databases, and verify they are on a dedicated partition.

If the mailbox databases are not on a dedicated partition, this is a finding.

Remediation:

Update the EDSP to specify the location where the Exchange Mailbox databases reside or verify that this information is documented by the organization.

Configure the mailbox databases on a dedicated partition.

Ensure the drive that its being moved to has enough space for the database and logs (if not moving the logs to their own partition). Consult the EDSP and ensure that this is done within a maintenance window as this will incur downtime for any users connected to this mailbox database. Ensure backups are not running at the time this needs to be done. If this server is in a Database Availability Group, this cannot be done until all replicated copies of that database are removed first. Then the move operation can be performed. Once completed, replicated copies can be recreated appropriately.

In an Exchange Management Shell, run the following (assuming copies of the database is removed if replicated or if it is a single copy database):

```
Move-DatabasePath -Identity "<name of database>" -EdbFilePath
"<drive>:\PathToDatabase\<MailboxDatabase.edb>" -LogFolderPath
"<drive>:\LogFolderPath\"
```

Example:

```
Move-DatabasePath -Identity "Database1" -EdbFilePath
"D:\MailboxDBs\Database1.edb" -LogFolderPath "D:\MailboxDBLogs\"
```

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

1.26 EX19-MB-000106 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internet-facing send connectors must specify a smart host.

```
GROUP ID: V-259670
RULE ID: SV-259670r961101
```

Rationale:

When identifying a "Smart Host" for the email environment, a logical Send connector is the preferred method.

A Smart Host acts as an internet-facing concentrator for other email servers. Appropriate hardening can be applied to the Smart Host, rather than at multiple locations throughout the enterprise.

Failure to identify a Smart Host could default to each email server performing its own lookups (potentially through protective firewalls). Exchange servers should not be internet facing and should therefore not perform any Smart Host functions. When the Exchange servers are internet facing, they must be configured to identify the internet-facing server that is performing the Smart Host function.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-SendConnector | Select-Object -Property Name, Identity, SmartHosts
```

Identify the internet-facing connectors.

For each Send connector, if the value of "SmartHosts" does not return the Smart Host IP address, this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-SendConnector -Identity <'IdentityName'> -SmartHosts <'IP Address of
Smart Host'> -DNSRoutingEnabled $false
```

Note: The <IdentityName> and <IP Address of Smart Host> values must be in quotes.

Repeat the procedure for each Send connector.

Additional Information:

CCI-001178 Provide additional data origin authentication artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

- NIST SP 800-53::SC-20
- NIST SP 800-53A::SC-20.1
- NIST SP 800-53 Revision 4::SC-20 a
- NIST SP 800-53 Revision 5::SC-20 a

1.27 EX19-MB-000115 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange mailboxes must be retained until backups are complete.

```
GROUP ID: V-259671
RULE ID: SV-259671r961128
```

Rationale:

Backup and recovery procedures are an important part of overall system availability and integrity. Complete backups reduce the chance of accidental deletion of important information and make it possible to have complete recoveries.

It is not uncommon for users to receive and delete messages in the scope of a single backup cycle. This setting ensures at least one backup has been run on the mailbox store before the message physically disappears. By enabling this setting, all messages written to recipients who have accounts on this store will reside in backups even if they have been deleted by the user before the backup has run.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-MailboxDatabase| Select-Object -Property Name, Identity,
RetainDeletedItemsUntilBackup
```

If the value of "RetainDeletedItemsUntilBackup" is not set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-MailboxDatabase -Identity <'IdentityName'> -RetainDeletedItemsUntilBackup
$true
```

Note: The <IdentityName> value must be in quotes.

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

1.28 EX19-MB-000116 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange email forwarding must be restricted.

```
GROUP ID: V-259672
RULE ID: SV-259672r961128
```

Rationale:

Auto-forwarded email accounts do not meet the requirement for digital signature and encryption of Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII) in accordance with DODI 8520.2 (reference ee) and DOD Director for Administration and Management memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information".

Use of forwarding set by an administrator interferes with nonrepudiation requirements that each end user be responsible for creation and destination of email data.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine any accounts that have been authorized to have email auto-forwarded.

Note: If email auto-forwarding is not being used, this check is not applicable.

Open the Exchange Management Shell and enter the following commands:

```
Get-Mailbox | Select-Object -Property Name, Identity, Forward*
```

Note: The asterisk (*) will grab both ForwardingAddress and ForwardingSMTPAddress.

If any user has a forwarding SMTP address and is not documented in the EDSP, this is a finding.

Note: If no remote SMTP domain matching the mail-enabled user or contact that allows forwarding is configured for users identified with a forwarding address, this function will not work properly.

Remediation:

Update the EDSP.

Open the Exchange Management Shell and enter the following command:

```
Set-Mailbox -Identity <'IdentityName'> -ForwardingSMTPAdddress $null
```

Note: The <IdentityName> value must be in quotes.

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

1.29 EX19-MB-000117 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange email-forwarding SMTP domains must be restricted.

```
GROUP ID: V-259673
RULE ID: SV-259673r961128
```

Rationale:

Auto-forwarded email accounts do not meet the requirement for digital signature and encryption of Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII) in accordance with DODI 8520.2 (reference ee) and DOD Director for Administration and Management memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information".

Use of forwarding set by an administrator interferes with nonrepudiation requirements that each end user be responsible for creation and destination of email data.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine any accounts that have been authorized to have email auto-forwarded.

Note: If email auto-forwarding is not being used, this check is not applicable (NA).

Open the Exchange Management Shell and enter the following commands:

```
Get-RemoteDomain | Select Name, Identity, DomainName, AutoForwardEnabled
|Format-List
```

If any domain for a user forwarding SMTP address is not documented in the EDSP, this is a finding.

Note: If no remote SMTP domain matching the mail-enabled user or contact that allows forwarding is configured for users identified with a forwarding address, this function will not work properly.

Remediation:

Update the EDSP to specify any accounts that have been authorized to have email auto-forwarded or verify that this information is documented by the organization.

For domains that are listed in the EDSP to allow AutoForwarding, open the Exchange Management Shell and enter the following command:

```
Set-RemoteDomain -Identity <RemoteDomainIdParameter>  -AutoForwardEnabled
$true
```

If the Remote Domain is NOT listed in the EDSP to allow for AutoForwarding, open the Exchange Management Shell and enter the following command:

```
Set-RemoteDomain -Identity [RemoteDomainIdentity] -AutoForwardingEnabled
$false
```

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

1.30 EX19-MB-000121 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange mailbox stores must mount at startup.

```
GROUP ID: V-259674
RULE ID: SV-259674r961152
```

Rationale:

Administrator responsibilities include the ability to react to unplanned maintenance tasks or emergency situations that may require Mailbox data manipulation. Occasionally, there may be a need to start the server with "unmounted" data stores if manual maintenance is being performed on them. Failure to uncheck the "do not mount on startup" condition will result in unavailability of mail services.

Correct configuration of this control will prevent unplanned outages due to being enabled. When maintenance is being performed, care should be taken to clear the check box upon task completion so mail stores are available to users (unmounted mailbox stores are not available to users).

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-MailboxDatabase | Select-Object -Property Name, Identity, MountAtStartup
```

If the value of "MountAtStartup" is not set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-MailboxDatabase -Identity <'IdentityName'> -MountAtStartup $true
```

Note: The <IdentityName> value must be in quotes.

Additional Information:

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

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

1.31 EX19-MB-000122 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange mail quota settings must not restrict receiving mail.

```
GROUP ID: V-259675
RULE ID: SV-259675r961152
```

Rationale:

Mail quota settings control the maximum sizes of a user's mailbox and the system's response if these limits are exceeded. Mailbox data that is not monitored against a quota increases the risk of mail loss due to filled disk space, which can also render the system unavailable.

Failure to allow mail receipt may impede users from receiving mission-critical data.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-MailboxDatabase | Select-Object -Property Name, Identity,
ProhibitSendReceiveQuota
```

If the value of "ProhibitSendReceiveQuota" is not set to "Unlimited", this is a finding.

or

If the value of "ProhibitSendReceiveQuota" is set to an alternate value and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-MailboxDatabase -Identity <'IdentityName'> -ProhibitSendReceiveQuota
Unlimited
```

Note: The <IdentityName> value must be in quotes.

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Additional Information:

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

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

1.32 EX19-MB-000123 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange mail quota settings must not restrict sending mail.

```
GROUP ID: V-259676
RULE ID: SV-259676r961152
```

Rationale:

Mail quota settings control the maximum sizes of a user's mailbox and the system's response if these limits are exceeded. Mailbox data that is not monitored against a quota increases the risk of mail loss due to filled disk space, which can also render the system unavailable. Multiple controls supply graduated levels of opportunity to respond before risking email service loss.

This control prohibits the user from sending an email when the mailbox limit reaches the prohibit send quota value.

Note: Best practice for this setting is to prohibit the user from sending email when the mailbox reaches 90 percent of capacity.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the value for the Prohibit Send Quota limit.

Open the Exchange Management Shell and enter the following command:

```
Get-MailboxDatabase | Select-Object -Property Name, Identity,
ProhibitSendQuota
```

If the value of "ProhibitSendQuota" is not set to the site's Prohibit Send Quota limit, this is a finding.

Remediation:

Update the EDSP to specify the value for the Prohibit Send Quota limit or verify that this information is documented by the organization.

Open the Exchange Management Shell and enter the following command:

```
Set-MailboxDatabase -Identity <'IdentityName'> -ProhibitSendQuota
<'QuotaLimit'>
```

Note: The <IdentityName> and <QuotaLimit> values must be in quotes.

Additional Information:

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

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

1.33 EX19-MB-000124 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange Message size restrictions must be controlled on Receive connectors.

```
GROUP ID: V-259677
RULE ID: SV-259677r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. For message size restrictions, multiple places exist to set or override inbound or outbound message size. Failure to control the configuration strategy can result in loss of data or system availability.

This setting enables the administrator to control the maximum message size on receive connectors. Using connectors to control size limits may necessitate applying message size limitations in multiple places, with the potential of introducing conflicts and impediments in the mail flow. Changing this setting at the connector overrides the global one. Therefore, if operational needs require it, the connector value may be set lower than the global value with the rationale documented in the Email Domain Security Plan (EDSP).

Audit:

Review the EDSP or document that contains this information.

Determine the global maximum message receive size and whether signoff with risk acceptance is documented for the Receive connector to have a different value.

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select-Object -Property Name, Identity, MaxMessageSize
```

Identify internet-facing connectors.

For each Receive connector, if the value of "MaxMessageSize" is not the same as the global value, this is a finding.

or

If "MaxMessageSize" is set to a numeric value different from the global value and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the global maximum message receive size and, if operationally necessary, to document signoff with risk acceptance for the receive connector to have a different value, or verify that this information is documented by the organization.

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -MaxMessageSize
<'MaxReceiveSize'>
```

Note: The <IdentityName> and <MaxReceiveSize> values must be in quotes.

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Repeat the procedure for each Receive connector.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.34 EX19-MB-000125 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange Receive Connector Maximum Hop Count must be 60.

```
GROUP ID: V-259678
RULE ID: SV-259678r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. This setting controls the maximum number of hops (email servers traversed) a message may take as it travels to its destination. Part of the original internet protocol implementation, the hop count limit prevents a message being passed in a routing loop indefinitely. Messages exceeding the maximum hop count are discarded undelivered.

Recent studies indicate that virtually all messages can be delivered in fewer than 60 hops. If the hop count is set too low, messages may expire before they reach their destinations. If the hop count is set too high, an undeliverable message may cycle between servers, raising the risk of network congestion.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the Max Hop Count value for Receive connectors.

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select-Object -Property Name, MaxHopCount
```

For each Receive connector, if the value of "MaxHopCount" is not set to "60", this is a finding.

or

If the value of "MaxHopCount" is set to a value other than "60" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the "MaxHopCount" value or verify that this information is documented by the organization.

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -MaxHopCount 60
```

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Repeat the procedure for each Receive connector.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.35 EX19-MB-000126 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange send connector connections count must be limited.

```
GROUP ID: V-259679
RULE ID: SV-259679r961155
```

Rationale:

The Exchange Send connector setting controls the maximum number of simultaneous outbound connections allowed for a given SMTP connector and can be used to throttle the SMTP service if resource constraints warrant it. If the limit is too low, connections may be dropped. If the limit is too high, some domains may use a disproportionate resource share, denying access to other domains. Appropriate tuning reduces risk of data delay or loss.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine the value for SMTP Server Maximum Outbound Connections.

Open the Exchange Management Shell and enter the following command:

```
Get-TransportService | Select-Object -Property Name, Identity,
MaxOutboundConnections
```

If the value of "MaxOutboundConnections" is not set to "1000", this is a finding.

or

If "MaxOutboundConnections" is set to a value other than "1000" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the "MaxOutboundConnections" value.

Open the Exchange Management Shell and enter the following command:

```
Set-TransportService -Identity <'IdentityName'> -MaxOutboundConnections 1000
```

Note: The <IdentityName> value must be in quotes.

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.36 EX19-MB-000127 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange receive connectors must control the number of recipients per message.

```
GROUP ID: V-259680
RULE ID: SV-259680r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations.

This configuration controls the maximum number of recipients who will receive a copy of a message at one time. This tunable value is related to throughput capacity and can enable the ability to optimize message delivery.

Note: There are two types of default Receive connectors:

Client Servername: Accepts SMTP connections from all non-MAPI clients, such as POP and IMAP. As POP and IMAP are not authorized for use in DOD, these should not be present. Their default value for "MaxRecipientsPerMessage" is "200".

Default Servername: Accepts connections from other Hub Transport servers and any Edge Transport servers. Their default value for "MaxRecipientsPerMessage" is "5000".

Audit:

Note: This requirement applies to IMAP4. IMAP Secure is not restricted and does not apply to this requirement.

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the Maximum Recipients per Message value.

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select-Object -Property Name, Identity,
MaxRecipientsPerMessage
```

For each Receive connector, evaluate the "MaxRecipientsPerMessage" value.

For each Receive connector, if the value of "MaxRecipientsPerMessage" is not set to "5000", this is a finding.

or

If the value of "MaxRecipientsPerMessage" is set to a value other than "5000" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the "MaxRecipientsPerMessage" value or verify that this information is documented by the organization.

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -MaxRecipientsPerMessage 5000
```

Note: The <IdentityName> value must be in quotes.

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Repeat the procedure for each Receive connector.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.37 EX19-MB-000128 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange message size restrictions must be controlled on send connectors.

```
GROUP ID: V-259681
RULE ID: SV-259681r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. For message size restrictions, multiple places exist to set or override inbound or outbound message size. Failure to control the configuration strategy can result in loss of data or system availability.

This setting enables the administrator to control the maximum message size on a Send connector. Using connectors to control size limits may necessitate applying message size limitations in multiple places, with the potential of introducing conflicts and impediments in the mail flow. Changing this setting at the connector overrides the global one. Therefore, if operational needs require it, the connector value may be set lower than the global value with the rationale documented in the Email Domain Security Plan (EDSP).

Audit:

Review the EDSP or document that contains this information.

Determine the maximum message send size.

Open the Exchange Management Shell and enter the following command:

```
Get-SendConnector | Select-Object -Property Name, Identity, MaxMessageSize
```

For each Send connector, if the value of "MaxMessageSize" is not the same as the global value, this is a finding.

or

If "MaxMessageSize" is set to a numeric value different from the maximum message send size value documented in the EDSP, this is a finding.

Remediation:

Update the EDSP to specify the "MaxMessageSize" value or verify that this information is documented by the organization.

Open the Exchange Management Shell and enter the following command:

```
Set-SendConnector -Identity <'IdentityName'> -MaxMessageSize <MaxSendSize>
```

Note: The <IdentityName> value must be in quotes.

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Repeat the procedures for each Send connector.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.38 EX19-MB-000129 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange global inbound message size must be controlled.

```
GROUP ID: V-259682
RULE ID: SV-259682r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. Message size limits should be set to 10 MB at most but often are smaller, depending on the organization. The key point in message size is that it should be set globally and should not be set to "unlimited". Selecting "unlimited" on "MaxReceiveSize" is likely to result in abuse and can contribute to excessive server disk space consumption.

Message size limits may also be applied on SMTP connectors, public folders, and on the user account under Active Directory (AD). Changes at these lower levels are discouraged, as the single global setting is usually sufficient. This practice prevents conflicts that could impact availability and simplifies server administration.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the global maximum message receive size.

Open the Exchange Management Shell and enter the following command:

```
Get-TransportConfig | Select-Object -Property Name, Identity, MaxReceiveSize
```

If the value of "MaxReceiveSize" is not set to "10MB", this is a finding.

or

If "MaxReceiveSize" is set to an alternate value and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the "MaxReceiveSize" value or verify that this information is documented by the organization.

Open the Exchange Management Shell and enter the following command:

```
Set-TransportConfig -MaxReceiveSize 10MB
```

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.39 EX19-MB-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange global outbound message size must be controlled.

```
GROUP ID: V-259683
RULE ID: SV-259683r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. Message size limits should be set to 10 MB at most but often are smaller, depending on the organization. The key point in message size is that it should be set globally and should not be set to "unlimited". Selecting "unlimited" on "MaxReceiveSize" is likely to result in abuse and can contribute to excessive server disk space consumption.

Message size limits may also be applied on send and receive connectors, public folders, and on the user account under Active Directory (AD). Changes at these lower levels are discouraged, as the single global setting is usually sufficient. This practice prevents conflicts that could impact availability and simplifies server administration.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the global maximum message send size.

Open the Exchange Management Shell and enter the following command:

```
Get-TransportConfig | Select-Object -Property Name, Identity, MaxSendSize
```

If the value of "MaxSendSize" is not set to "10MB", this is a finding.

or

If "MaxSendSize" is set to an alternate value and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the "MaxSendSize" value or verify that this information is documented by the organization.

Open the Exchange Management Shell and enter the following command:

```
Set-TransportConfig -MaxSendSize 10MB
```

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.40 EX19-MB-000131 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange Outbound Connection Limit per Domain Count must be controlled.

```
GROUP ID: V-259684
RULE ID: SV-259684r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. This configuration controls the maximum number of simultaneous outbound connections from a domain as a delivery tuning mechanism. If the limit is too low, connections may be dropped. If the limit is too high, some domains may use a disproportionate resource share, denying access to other domains. Appropriate tuning reduces risk of data delay or loss.

By default, a limit of 20 simultaneous outbound connections from a domain should be sufficient. The value may be adjusted if justified by local site conditions.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the value for Maximum Outbound Domain Connections.

Open the Exchange Management Shell and enter the following command:

```
Get-TransportService | Select-Object -Property Name, Identity,
MaxPerDomainOutboundConnections
```

If the value of "MaxPerDomainOutboundConnections" is not set to "20", this is a finding.

or

If "MaxPerDomainOutboundConnections" is set to a value other than "20" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the "MaxPerDomainOutboundConnection" value or verify that this information is documented by the organization.

Open the Exchange Management Shell and enter the following command:

```
Set-TransportService -Identity <'IdentityName'> -
MaxPerDomainOutboundConnections 20
```

Note: The <IdentityName> value must be in quotes.

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.41 EX19-MB-000132 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange Outbound Connection Timeout must be 10 minutes or less.

```
GROUP ID: V-259685
RULE ID: SV-259685r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. This configuration controls the number of idle minutes before the connection is dropped. It works in conjunction with the Maximum Outbound Connections Count setting.

Once established, connections may incur delays in message transfer. The default of 10 minutes is a reasonable window in which to resume activities without maintaining idle connections for excessive intervals. If the timeout period is too long, idle connections may be maintained for unnecessarily long time periods, preventing new connections from being established. Sluggish connectivity increases the risk of lost data. A value of "10" or less is optimal.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the Connection Timeout value.

Open the Exchange Management Shell and enter the following command:

```
Get-SendConnector | Select-Object -Property Name, Identity,
ConnectionInactivityTimeOut
```

For each Send connector, if the value of "ConnectionInactivityTimeOut" is not set to "00:10:00", this is a finding.

or

If "ConnectionInactivityTimeOut" is set to a value other than "00:10:00" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the "ConnectionInactivityTimeOut" value.

Open the Exchange Management Shell and enter the following command:

```
Set-SendConnector -Identity <'IdentityName'> -ConnectionInactivityTimeOut
00:10:00
```

Note: The <IdentityName> value must be in quotes.

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.42 EX19-MB-000134 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Exchange servers must have an approved DOD email-aware virus protection software installed.

```
GROUP ID: V-259686
RULE ID: SV-259686r961161
```

Rationale:

With the proliferation of trojans, viruses, and spam attaching themselves to email messages (or attachments), it is necessary to have capable email-aware antivirus (AV) products to scan messages and identify any resident malware. Because email messages and their attachments are formatted to the MIME standard, a flat-file AV scanning engine is not suitable for scanning email message stores.

Email-aware antivirus engines must be Exchange 2019 compliant. Competent email scanners will have the ability to scan mail stores, attachments (including zip or other archive files) and mail queues and to issue warnings or alerts if malware is detected. As with other AV products, a necessary feature to include is the ability for automatic updates.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine the antivirus strategy.

Verify the email-aware antivirus scanner product is Exchange 2019 compatible and DOD approved.

If email servers are using an email-aware antivirus scanner product that is not DOD approved and Exchange 2019 compatible, this is a finding.

Remediation:

Update the EDSP to specify the organization's antivirus strategy.

Install and configure a DOD-approved compatible Exchange 2019 email-aware antivirus scanner product.

Additional Information:

CCI-001308 Automatically update spam protection mechanisms on an organization-defined frequency.

- NIST SP 800-53::SI-8 (2)
- NIST SP 800-53A::SI-8 (2).1
- NIST SP 800-53 Revision 4::SI-8 (2)
- NIST SP 800-53 Revision 5::SI-8 (2)

1.43 EX19-MB-000135 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internal receive connectors must not allow anonymous connections.

```
GROUP ID: V-259687
RULE ID: SV-259687r961161
```

Rationale:

This control is used to limit the servers that may use this server as a relay. If a Simple Mail Transport Protocol (SMTP) sender does not have a direct connection to the internet (for example, an application that produces reports to be emailed), it will need to use an SMTP Receive connector that does have a path to the internet (for example, a local email server) as a relay.

SMTP relay functions must be protected so third parties are not able to hijack a relay service for their own purposes. Most commonly, hijacking of relays is done by spammers to disguise the source of their messages and may also be used to cover the source of more destructive attacks.

Relays can be restricted in one of three ways: by blocking relays (restrict to a blank list of servers), by restricting use to lists of valid servers, or by restricting use to servers that can authenticate. Because authenticated connections are the most secure for SMTP Receive connectors, it is recommended that relays allow only servers that can authenticate.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select-Object -Property Name, Identity,
PermissionGroups |Format-List
```

For each Receive connector, if the value of "PermissionGroups" is "AnonymousUsers" for any receive connector, this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity ['IdentityName'] -PermissionGroups and enter a
valid value user group.
```

Note: The <IdentityName> value must be in quotes.

Example:

```
Set-ReceiveConnector -Identity <'IdentityName'> -PermissionGroups
ExchangeUsers
```

Repeat the procedures for each Receive connector. This will remove the AnonymousUsers value simultaneously.

Additional Information:

CCI-001308 Automatically update spam protection mechanisms on an organization-defined frequency.

- NIST SP 800-53::SI-8 (2)
- NIST SP 800-53A::SI-8 (2).1
- NIST SP 800-53 Revision 4::SI-8 (2)
- NIST SP 800-53 Revision 5::SI-8 (2)

1.44 EX19-MB-000137 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have anti-spam filtering installed.

```
GROUP ID: V-259689
RULE ID: SV-259689r961161
```

Rationale:

Originators of spam messages are constantly changing their techniques to defeat spam countermeasures; therefore, spam software must be constantly updated to address the changing threat. A manual update procedure is labor intensive and does not scale well in an enterprise environment. This risk may be mitigated by using an automatic update capability. Spam protection mechanisms include, for example, signature definitions, rule sets, and algorithms.

Exchange 2019 provides both anti-spam and anti-malware protection out of the box. The Exchange 2019 anti-spam and anti-malware product capabilities are limited but still provide some protection.

Audit:

Review the Email Domain Security Plan (EDSP).

Note: If using another DOD-approved anti-spam product for email or a DOD-approved email gateway spamming device, such as Enterprise Email Security Gateway (EEMSG), this is not applicable.

Open the Exchange Management Shell and enter the following command:

```
Get-ContentFilterConfig |Select-Object -Property Name, Enabled |Format-Table
```

If no value is returned, this is a finding.

Remediation:

Update the EDSP with the anti-spam mechanism used.

Install the AntiSpam module.

Open the Exchange Management Shell and enter the following command:

```
& $env:ExchangeInstallPath\Scripts\Install-AntiSpamAgents.ps1
```

Additional Information:

CCI-001308 Automatically update spam protection mechanisms on an organization-defined frequency.

- NIST SP 800-53::SI-8 (2)
- NIST SP 800-53A::SI-8 (2).1
- NIST SP 800-53 Revision 4::SI-8 (2)
- NIST SP 800-53 Revision 5::SI-8 (2)

1.45 EX19-MB-000136 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange external/internet-bound automated response messages must be disabled.

```
GROUP ID: V-259688
RULE ID: SV-259688r961161
```

Rationale:

Spam originators, in an effort to refine mailing lists, sometimes monitor transmissions for automated bounce-back messages. Automated messages include such items as "Out of Office" responses, nondelivery messages, and automated message forwarding.

Automated bounce-back messages can be used by a third party to determine if users exist on the server. This can result in the disclosure of active user accounts to third parties, paving the way for possible future attacks.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-RemoteDomain | Select-Object -Property Name, DomainName, Identity,
AllowedOOFType
```

If the value of "AllowedOOFType" is not set to "InternalLegacy", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-RemoteDomain -Identity <'IdentityName'> -AllowedOOFType 'InternalLegacy'
```

Note: The <IdentityName> and InternalLegacy values must be in quotes.

Additional Information:

CCI-001308 Automatically update spam protection mechanisms on an organization-defined frequency.

- NIST SP 800-53::SI-8 (2)
- NIST SP 800-53A::SI-8 (2).1
- NIST SP 800-53 Revision 4::SI-8 (2)
- NIST SP 800-53 Revision 5::SI-8 (2)

1.46 EX19-MB-000138 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have anti-spam filtering enabled.

```
GROUP ID: V-259690
RULE ID: SV-259690r961161
```

Rationale:

Originators of spam messages are constantly changing their techniques to defeat spam countermeasures; therefore, spam software must be constantly updated to address the changing threat. A manual update procedure is labor intensive and does not scale well in an enterprise environment. This risk may be mitigated by using an automatic update capability. Spam protection mechanisms include, for example, signature definitions, rule sets, and algorithms.

Exchange 2019 provides both anti-spam and anti-malware protection out of the box. The Exchange 2019 anti-spam and anti-malware product capabilities are limited but still provide some protection.

Audit:

Review the Email Domain Security Plan (EDSP).

Note: If using another DOD-approved anti-spam product for email or a DOD-approved email gateway spamming device, such as Enterprise Email Security Gateway (EEMSG), this is not applicable.

Open the Exchange Management Shell and enter the following command:

```
Get-ContentFilterConfig | Select-Object -Property Name, Enabled|Format-Table;
Get-SenderFilterConfig |Select-Object -Property Name, Enabled |Format-Table;
Get-SenderIDConfig |Select-Object -Property Name, Enabled |Format-Table;
Get-SenderReputationConfig |Select-Object -Property Name, Enabled |Format-
Table
```

If any of the above values returned are not set to "True", this is a finding.

Remediation:

Update the EDSP with the anti-spam mechanism used.

Open the Exchange Management Shell and enter the following command for any values that were not set to "True":

```
Set-ContentFilterConfig -Enabled $true
Set-SenderFilterConfig -Enabled $true
Set-SenderIDConfig -Enabled $true
Set-SenderReputationConfig -Enabled $true
```

Additional Information:

CCI-001308 Automatically update spam protection mechanisms on an organization-defined frequency.

- NIST SP 800-53::SI-8 (2)
- NIST SP 800-53A::SI-8 (2).1
- NIST SP 800-53 Revision 4::SI-8 (2)
- NIST SP 800-53 Revision 5::SI-8 (2)

1.47 EX19-MB-000139 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have anti-spam filtering configured.

```
GROUP ID: V-259691
RULE ID: SV-259691r961161
```

Rationale:

Originators of spam messages are constantly changing their techniques to defeat spam countermeasures; therefore, spam software must be constantly updated to address the changing threat. A manual update procedure is labor intensive and does not scale well in an enterprise environment. This risk may be mitigated by using an automatic update capability. Spam protection mechanisms include, for example, signature definitions, rule sets, and algorithms.

Exchange 2019 provides both anti-spam and anti-malware protection out of the box. The Exchange 2019 anti-spam and anti-malware product capabilities are limited but still provide some protection.

Audit:

Review the Email Domain Security Plan (EDSP).

Note: If using another DOD-approved anti-spam product for email or a DOD-approved email gateway spamming device, such as Enterprise Email Security Gateway (EEMSG), this is not applicable.

Determine the internal SMTP servers.

Open the Exchange Management Shell and enter the following command:

```
Get-TransportConfig | Format-List InternalSMTPServers
```

If any internal SMTP server IP address returned does not reflect the list of accepted SMTP server IP addresses, this is a finding.

Remediation:

Note: Configure the IP addresses of every internal SMTP server. If the Mailbox server is the only SMTP server running the anti-spam agents, configure the IP address of the Mailbox server.

Update the EDSP with the anti-spam mechanism used.

Open the Exchange Management Shell and enter the following command:

Single SMTP server address:

```
Set-TransportConfig -InternalSMTPServers @{Add='<ip address1>'}
```

Multiple SMTP server addresses:

```
Set-TransportConfig -InternalSMTPServers @{Add='<ip address1>','<ip
address2>'}
```

Additional Information:

CCI-001308 Automatically update spam protection mechanisms on an organization-defined frequency.

- NIST SP 800-53::SI-8 (2)
- NIST SP 800-53A::SI-8 (2).1
- NIST SP 800-53 Revision 4::SI-8 (2)
- NIST SP 800-53 Revision 5::SI-8 (2)

1.48 EX19-MB-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must not send automated replies to remote domains.

```
GROUP ID: V-259692
RULE ID: SV-259692r961161
```

Rationale:

Attackers can use automated messages to determine whether a user account is active, in the office, traveling, and so on. An attacker might use this information to conduct future attacks. Remote users will not receive automated "Out of Office" delivery reports. This setting can be used to determine if all the servers in the organization can send "Out of Office" messages.

Audit:

Note: Automated replies to .mil or .gov sites are allowed.

Open the Exchange Management Shell and enter the following command:

```
Get-RemoteDomain | Select-Object -Property Name, Identity, AutoReplyEnabled
```

If the value of "AutoReplyEnabled" is set to "True" and is configured to only reply to .mil or .gov sites, this is not a finding.

If the value of "AutoReplyEnabled" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-RemoteDomain -Identity <'IdentityName'> -AutoReplyEnabled $false
```

Note: The <IdentityName> value must be in quotes.

Additional Information:

CCI-001308 Automatically update spam protection mechanisms on an organization-defined frequency.

- NIST SP 800-53::SI-8 (2)
- NIST SP 800-53A::SI-8 (2).1
- NIST SP 800-53 Revision 4::SI-8 (2)
- NIST SP 800-53 Revision 5::SI-8 (2)

1.49 EX19-MB-000142 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange Global Recipient Count Limit must be set.

```
GROUP ID: V-259693
RULE ID: SV-259693r961161
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. The Global Recipient Count Limit field is used to control the maximum number of recipients that can be specified in a single message sent from this server. Its primary purpose is to minimize the chance of an internal sender spamming other recipients, since spam messages often have a large number of recipients. Spam prevention can originate from both outside and inside organizations. While inbound spam is evaluated as it arrives, controls such as this one help prevent spam that might originate inside the organization.

The Recipient Count Limit is global to the Exchange implementation. Lower-level refinements are possible; however, in this configuration strategy, setting the value once at the global level facilitates a more available system by eliminating potential conflicts among multiple settings. A value of less than or equal to "5000" is probably larger than is needed for most organizations but is small enough to minimize usefulness to spammers and is easily handled by Exchange. An unexpanded distribution is handled as one recipient. Specifying "unlimited" may result in abuse.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine the global maximum message recipient count.

Open the Exchange Management Shell and enter the following command:

```
Get-TransportConfig | Select-Object -Property Name, Identity,
MaxRecipientEnvelopeLimit
```

If the value of "MaxRecipientEnvelopeLimit" is not set to "5000", this is a finding.

or

If "MaxRecipientEnvelopeLimit" is set to an alternate value and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the global maximum message recipient count.

```
Set-TransportConfig -MaxRecipientEnvelopeLimit 5000
```

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Restart the Microsoft Exchange Information Store service.

Additional Information:

CCI-001308 Automatically update spam protection mechanisms on an organization-defined frequency.

- NIST SP 800-53::SI-8 (2)
- NIST SP 800-53A::SI-8 (2).1
- NIST SP 800-53 Revision 4::SI-8 (2)
- NIST SP 800-53 Revision 5::SI-8 (2)

1.50 EX19-MB-000146 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange antimalware agent must be enabled and configured.

```
GROUP ID: V-259694
RULE ID: SV-259694r1015276
```

Rationale:

Microsoft Exchange 2019 offers built-in antimalware protection for messages going through the transport pipeline. When enabled, the default settings are configured to automatically update.

Exchange's built-in Malware Agent is not designed to address all malicious code protection workloads. This workload is best handled by third-party antivirus and intrusion prevention software.

Sites must use an approved DOD scanner. Exchange Malware software has a limited scanning capability and does not scan files that are downloaded, opened, or executed.

Audit:

Open the Exchange Management Shell and run the following cmdlets:

```
Get-TransportAgent "Malware Agent"
```

If the identity "Malware Agent" is not set to "Enabled", this is a finding.

Remediation:

Open the Exchange Management Shell and run the following command:

```
& $env:ExchangeInstallPath\Scripts\Enable-AntimalwareScanning.ps1
```

This will automatically enable the anti-malware agent. After the script completes, run the following cmdlet to complete the process:

```
Restart-Service MSExchangeTransport
```

This may take up to 10 minutes to take effect.

Additional Information:

CCI-004964 Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy.

- NIST SP 800-53 Revision 5::SI-3 b

CCI-002624 Configure malicious code protection mechanisms to perform real-time scans of files from external sources at endpoint; and/or network entry and exit points as the files are downloaded, opened, or executed in accordance with organizational policy.

- NIST SP 800-53 Revision 4::SI-3 c 1
- NIST SP 800-53 Revision 5::SI-3 c 1

CCI-001247 The information system automatically updates malicious code protection mechanisms.

- NIST SP 800-53::SI-3 (2)
- NIST SP 800-53A::SI-3 (2).1
- NIST SP 800-53 Revision 4::SI-3 (2)

1.51 EX19-MB-000147 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange malware scanning agent must be configured for automatic updates.

```
GROUP ID: V-259695
RULE ID: SV-259695r1015277
```

Rationale:

Antimalware protection in Exchange Server 2019 helps combat viruses and spyware in an email messaging environment. Viruses infect other programs and data, and they spread throughout computer looking for programs to infect. Spyware gathers personal information (for example, sign-in information and personal data) and sends it back to its author.

The antimalware protection in Exchange Server was introduced in Exchange 2013 and is provided by the Transport agent named Malware Agent. The agent scans messages as they travel through the Transport service on a Mailbox server.

To ensure increased effectiveness of the Malware Agent, ensuring its signatures are automatically updated is imperative. Not doing so can lead to system compromise.

The Malware agent is installed during the initial installation of Microsoft Exchange server and if installed, is set for automatic updates by default.

Audit:

In Exchange Management shell, run the following cmdlet:

```
Get-MalwareFilteringServer |Select-Object -Property Name, *Update*
```

If the property "Update frequency" is not set, this is a finding.

If the Malware agent is not installed, then this is not applicable.

Remediation:

In an elevated Exchange management shell, run the following cmdlet:

```
Set-MalwareFilteringServer -Identity <Identity> -UpdateFrequency <integer>
```

Where <Identity> is the name of the Exchange Server and is the update frequency (in minutes).

Refer to the Enterprise Domain Security Plan (EDSP) for the update cadence that best aligns with the user's organization.

Additional Information:

CCI-004964 Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy.

- NIST SP 800-53 Revision 5::SI-3 b

CCI-001247 The information system automatically updates malicious code protection mechanisms.

- NIST SP 800-53::SI-3 (2)
- NIST SP 800-53A::SI-3 (2).1
- NIST SP 800-53 Revision 4::SI-3 (2)

1.52 EX19-MB-000158 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange receive connector timeout must be limited.

```
GROUP ID: V-259697
RULE ID: SV-259697r961221
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning. This configuration controls the number of idle minutes before the connection is dropped. It works in conjunction with the Maximum Inbound Connections Count setting.

Connections, once established, may incur delays in message transfer. If the timeout period is too long, there is risk that idle connections may be maintained for unnecessarily long time periods, preventing new connections from being established.

Audit:

Review the Email Domain Security Plan (EDSP) and determine the Connection Timeout value.

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select-Object -Property Name, Identity,
ConnectionTimeout
```

For each Receive connector, if the value of "ConnectionTimeout" is not set to "00:10:00", this is a finding.

or

If "ConnectionTimeout" is set to other than "00:10:00" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to specify the Connection Timeout value.

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -ConnectionTimeout 00:10:00
```

Note: The <IdentityName> value must be in quotes.

or

Enter the value as identified by the EDSP that has obtained a signoff with risk acceptance.

Additional Information:

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.53 EX19-MB-000194 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange application directory must be protected from unauthorized access.

```
GROUP ID: V-259699
RULE ID: SV-259699r1015278
```

Rationale:

Default product installations may provide more generous access permissions than are necessary to run the application. By examining and tailoring access permissions to provide the least amount of privilege possible more closely, attack vectors that align with user permissions are less likely to access more highly secured areas.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the authorized groups and users that have access to the Exchange application directories.

Verify the access permissions on the directory match the access permissions listed in the EDSP.

If any group or user has different access permissions, this is a finding.

Note: The default installation directory is \Program Files\Microsoft\Exchange Server\V15.

Remediation:

Update the EDSP to specify the authorized groups and users that have access to the Exchange application directories or verify that this information is documented by the organization.

Navigate to the Exchange application directory and remove or modify the group or user access permissions.

Note: The default installation directory is \Program Files\Microsoft\Exchange Server\V15.

Additional Information:

CCI-003980 Allow user installation of software only with explicit privileged status.

- NIST SP 800-53 Revision 5::CM-11 (2)

CCI-001812 The information system prohibits user installation of software without explicit privileged status.

- NIST SP 800-53 Revision 4::CM-11 (2)

1.54 EX19-MB-000173 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Role-Based Access Control must be defined for privileged and nonprivileged users.

```
GROUP ID: V-259698
RULE ID: SV-259698r961353
```

Rationale:

Role Based Access Control (RBAC) is the permissions model used in Microsoft Exchange Server 2013, 2016, and 2019. With RBAC, there is no need to modify and manage access control lists (ACLs), which was done in Exchange Server 2007. ACLs created several challenges in Exchange 2007, such as modifying ACLs without causing unintended consequences, maintaining ACL modifications through upgrades, and troubleshooting problems that occurred due to using ACLs in a nonstandard way.

RBAC enables users to control, at both broad and granular levels, what administrators and end-users can do. RBAC also enables users to more closely align the roles assigned to users and administrators to the actual roles they hold within the organization. In Exchange 2007, the server permissions model applied only to the administrators who managed the Exchange 2007 infrastructure. Starting with Exchange 2013, RBAC now controls both the administrative tasks that can be performed and the extent to which users can now administer their own mailbox and distribution groups.

Audit:

Review the Email Domain Security Plan (EDSP) to verify which users should be in each built-in RBAC management role group.

If this is not found, this is a finding.

Remediation:

Update the EDSP and define which users should and should not have elevated privileges within the organization.

Follow the rule of least privilege and ensure that administrators are given just enough access to complete their job.

Referenced Document: https://docs.microsoft.com/en-us/exchange/understanding-management-role-groups-exchange-2013-help?view=exchserver-2019

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)

1.55 EX19-MB-000196 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

An Exchange software baseline copy must exist.

```
GROUP ID: V-259700
RULE ID: SV-259700r961461
```

Rationale:

Exchange software, as with other application software installed on a host system, must be included in a system baseline record and periodically reviewed; otherwise, unauthorized changes to the software may not be discovered. This effort is a vital step to securing the host and the applications, as it is the only method that may provide the ability to detect and recover from otherwise undetected changes, such as those that result from worm or bot intrusions.

The Exchange software and configuration baseline is created and maintained for comparison during scanning efforts. Operational procedures must include baseline updates as part of configuration management tasks that change the software and configuration.

Audit:

Review the Email Domain Security Plan (EDSP) or document that contains this information.

Determine the software baseline.

Review the application software baseline procedures and implementation artifacts.

Note the list of files and directories included in the baseline procedure for completeness.

If an email software copy exists to serve as a baseline and is available for comparison during scanning efforts, this is not a finding.

Remediation:

Update the EDSP to specify the software baseline, procedures, and implementation artifacts or verify that this information is documented by the organization.

Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

1.56 EX19-MB-000197 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange software must be monitored for unauthorized changes.

```
GROUP ID: V-259701
RULE ID: SV-259701r1015279
```

Rationale:

Monitoring software files for changes against a baseline on a regular basis may help detect the possible introduction of malicious code on a system.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine whether the site monitors system files (e.g., *.exe, *.bat, *.com, *.cmd, and *.dll) on servers for unauthorized changes against a baseline on a weekly basis.

If software files are not monitored for unauthorized changes, this is a finding.

Note: An approved and properly configured solution will contain both a list of baselines that includes all system file locations and a file comparison task that is scheduled to run at least weekly.

Remediation:

Update the EDSP to specify that the organization monitors system files on servers for unauthorized changes against a baseline on a weekly basis or verify that this information is documented by the organization.

Monitor the software files (e.g., *.exe, *.bat, *.com, *.cmd, and *.dll) on Exchange servers for unauthorized changes against a baseline on a weekly basis.

Note: This can be done with the use of various monitoring tools.

Additional Information:

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-001814 The Information system supports auditing of the enforcement actions.

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

1.57 EX19-MB-000198 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange services must be documented, and unnecessary services must be removed or disabled.

```
GROUP ID: V-259702
RULE ID: SV-259702r961470
```

Rationale:

Unneeded but running services offer attackers an enhanced attack profile, and attackers are constantly watching to discover open ports with running services. By analyzing and disabling unneeded services, the associated open ports become unresponsive to outside queries, and servers become more secure as a result.

Exchange Server has role-based server deployment to enable protocol path control and logical separation of network traffic types.

For example, a server implemented in the Client Access role (i.e., Outlook Web App [OWA]) is configured and tuned as a web server using web protocols. A client access server exposes only web protocols (HTTP/HTTPS), enabling system administrators to optimize the protocol path and disable all services unnecessary for Exchange web services. Similarly, servers created to host mailboxes are dedicated to that task and must operate only the services needed for mailbox hosting. (Exchange servers must also operate some web services, but only to the degree that Exchange requires the IIS engine in order to function).

Because Post Office Protocol 3 (POP3) and Internet Message Access Protocol 4 (IMAP4) clients are not included in the standard desktop offering, they must be disabled. While IMAP4 is restricted, IMAP Secure is not restricted and does not apply to this requirement.

Audit:

Review the Email Domain Security Plan (EDSP).

Note: Required services will vary among organizations depending on the role of the individual system. Organizations will develop their own list of services, which will be documented and justified with the information system security officer (ISSO). The site's list will be provided for any security review. Services that are common to multiple systems can be addressed in one document. Exceptions for individual systems should be identified separately by system.

Open a Windows PowerShell and enter the following command:

```
Get-Service | Where-Object {$_.status -eq 'running'}
```

Note: The command returns a list of installed services and the status of that service.

If the services required are not documented in the EDSP, this is a finding.

If any undocumented or unnecessary services are running, this is a finding.

Remediation:

Update the EDSP to specify the services required for the system to function.

Remove or disable any services that are not required.

Additional Information:

CCI-001762 Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.58 EX19-MB-000203 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Outlook Anywhere clients must use NTLM authentication to access email.

```
GROUP ID: V-259703
RULE ID: SV-259703r961494
```

Rationale:

Identification and authentication provide the foundation for access control. Access to email services applications require NTLM authentication. Outlook Anywhere, if authorized for use by the site, must use NTLM authentication when accessing email.

Note: There is a technical restriction in Exchange Outlook Anywhere that requires a direct SSL connection from Outlook to the Certificate Authority (CA) server. There is also a constraint where Microsoft supports that the CA server must participate in the Active Director (AD) domain inside the enclave. For this reason, Outlook Anywhere must be deployed only for enclave-sourced Outlook users.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-OutlookAnywhere

Get-OutlookAnywhere | Select-Object -Property Name, Identity,
InternalClientAuthenticationMethod, ExternalClientAuthenticationMethod
```

If the value of "InternalClientAuthenticationMethod" and the value of "ExternalClientAuthenticationMethod" are not set to NTLM, this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

For InternalClientAuthenticationMethod:

```
Set-OutlookAnywhere -Identity '<IdentityName'> -
InternalClientAuthenticationMethod NTLM
```

For ExternalClientAuthenticationMethod:

```
Set-OutlookAnywhere -Identity '<IdentityName'> -
ExternalClientAuthenticationMethod NTLM
```

Additional Information:

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

1.59 EX19-MB-000229 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange email application must not share a partition with another application.

```
GROUP ID: V-259704
RULE ID: SV-259704r961608
```

Rationale:

In the same way that added security layers can provide a cumulative positive effect on security posture, multiple applications can provide a cumulative negative effect. A vulnerability and subsequent exploit to one application can lead to an exploit of other applications sharing the same security context. For example, an exploit to a web server process that leads to unauthorized administrative access to the host system can most likely lead to a compromise of all applications hosted by the same system.

Email services should be installed on a partition that does not host other applications. Email services should never be installed on a Domain Controller/Directory Services server.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine if the directory Exchange is installed:

1. Open Windows Explorer.
2. Navigate to where Exchange is installed.

If Exchange resides on a directory or partition other than that of the operating system and does not have other applications installed (unless approved by the Information System Security Officer [ISSO]), this is not a finding.

Remediation:

Update the EDSP with the location of where Exchange is installed.

Install Exchange on a dedicated application directory or partition separate than that of the operating system.

Additional Information:

CCI-002530 Maintain a separate execution domain for each executing system process.

- NIST SP 800-53 Revision 4::SC-39
- NIST SP 800-53 Revision 5::SC-39

1.60 EX19-MB-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must not send delivery reports to remote domains.

```
GROUP ID: V-259705
RULE ID: SV-259705r961620
```

Rationale:

Attackers can use automated messages to determine whether a user account is active, in the office, traveling, and so on. An attacker might use this information to conduct future attacks. Ensure that delivery reports to remote domains are disabled. Before enabling this setting, first configure a remote domain using the Exchange Management Console (EMC) or the New-RemoteDomain cmdlet.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-RemoteDomain | Select-Object -Property Identity, DeliveryReportEnabled
```

If the value of "DeliveryReportEnabled" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-RemoteDomain -Identity <'IdentityName'> -DeliveryReportEnabled $false
```

Note: The <IdentityName> value must be in quotes.

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.61 EX19-MB-000231 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must not send nondelivery reports to remote domains.

```
GROUP ID: V-259706
RULE ID: SV-259706r961620
```

Rationale:

Attackers can use automated messages to determine whether a user account is active, in the office, traveling, and so on. An attacker might use this information to conduct future attacks. Ensure that nondelivery reports to remote domains are disabled. Before enabling this setting, first configure a remote domain using the Exchange Management Console (EMC) or the New-RemoteDomain cmdlet.

Audit:

Note: For the purpose of this requirement, "remote" refers to those domains external to the DODIN, whether classified or unclassified. NDRs between DODIN networks is permitted.

Open the Exchange Management Shell and enter the following command:

```
Get-RemoteDomain | Select-Object -Property Name, Identity, NDREnabled
```

If the value of "NDREnabled" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-RemoteDomain -Identity <'IdentityName'> -NDREnabled $false
```

Note: The <IdentityName> value must be in quotes.

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.62 EX19-MB-000232 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange SMTP automated banner response must not reveal server details.

```
GROUP ID: V-259707
RULE ID: SV-259707r961620
```

Rationale:

Automated connection responses occur as a result of FTP or Telnet connections when connecting to those services. They report a successful connection by greeting the connecting client and stating the name, release level, and (often) additional information regarding the responding product. While useful to the connecting client, connection responses can also be used by a third party to determine operating system or product release levels on the target server. The result can include disclosure of configuration information to third parties, paving the way for possible future attacks. For example, when querying the SMTP service on port 25, the default response looks similar to this one:

220 exchange.mydomain.org Microsoft ESMTP MAIL Service ready at Tuesday, 23 Nov 2021 13:43:00 -0500

Changing the response to hide local configuration details reduces the attack profile of the target.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select-Object -Property Name, Identity, Banner
```

For each Receive connector, if the value of "Banner" is not set to "220 SMTP Server Ready", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -Banner '220 SMTP Server
Ready'
```

Note: The <IdentityName> and 220 SMTP Server Ready values must be in quotes.

Repeat the procedures for each Receive connector.

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.63 EX19-MB-000233 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internal send connectors must use an authentication level.

```
GROUP ID: V-259708
RULE ID: SV-259708r961620
```

Rationale:

The Simple Mail Transfer Protocol (SMTP) connector is used by Exchange to send and receive messages from server to server. Several controls work together to provide security between internal servers. This setting controls the encryption method used for communications between servers. With this feature enabled, only servers capable of supporting Transport Layer Security (TLS) will be able to send and receive mail within the domain.

The use of secure communication prevents eavesdroppers from reading or modifying communications between mail clients and servers. While sensitive message bodies should be encrypted by the sender at the client, requiring a secure connection from server to server adds protection by encrypting the sender and recipient information that cannot be encrypted by the sender.

Individually, channel security and encryption can be compromised by attackers. Used together, email becomes a more difficult target, and security is heightened. Failure to enable this feature gives eavesdroppers an opportunity to read or modify messages between servers.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-SendConnector | Select-Object -Property Name, Identity, TlsAuthLevel
```

For each Send connector, if the value of "TlsAuthLevel" is not set to "DomainValidation", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-SendConnector -Identity <'IdentityName'> -TlsAuthLevel DomainValidation
```

Note: The <IdentityName> value must be in quotes.

Repeat the procedure for each Send connector.

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.64 EX19-MB-000234 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must provide mailbox databases in a highly available and redundant configuration.

```
GROUP ID: V-259709
RULE ID: SV-259709r961620
```

Rationale:

Exchange Server mailbox databases and any data contained in those mailboxes should be protected. This can be accomplished by configuring Mailbox servers and databases for high availability and site resilience.

A database availability group (DAG) is a component of the Mailbox server high availability and site resilience framework built into Microsoft Exchange Server 2019. A DAG is a group of Mailbox servers that hosts a set of databases and provides automatic database-level recovery from failures that affect individual servers or databases.

A DAG is a boundary for mailbox database replication and database and server switchovers and failovers.

Any server in a DAG can host a copy of a mailbox database from any other server in the DAG. When a server is added to a DAG, it works with the other servers in the DAG to provide automatic recovery from failures that affect mailbox databases, such as a disk, server, or network failure.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine if a Database Availability Group exists.

From Exchange Admin Center:

1. In the pane on the left, navigate to "servers".
2. In the pane on the right, navigate to the "database availability groups" tab.
3. Verify a database availability group is configured with member servers.

If two or more member servers are not listed, this is a finding.
From Exchange PowerShell, run the following cmdlet:

```
Get-DatabaseAvailabilityGroup
```

If no DatabaseAvailabilityGroup is listed or a Database Availability Group is listed but has no member servers, this is a finding.

Determine if the Exchange Mailbox databases are using redundancy.

From Exchange Admin Center:

1. In the pane on the left, navigate to "servers".
2. In the pane on the right, navigate to the "databases" tab.
3. For each database, check the column "SERVERS WITH COPIES".

Unless specified in the EDSP, if the "SERVERS WITH COPIES" column does not have two or more servers listed, this is a finding.
From Exchange PowerShell, run the following cmdlet:

```
Get-MailboxDatabaseCopyStatus -Identity <DatabaseName>
```

Unless specified in the EDSP, if the output of this cmdlet does not show more than one copy, this is a finding.

Remediation:

Update the EDSP to specify how Exchange Mailbox databases use redundancy.

Add two or more Mailbox servers to the database availability group.

Add a database copy to one or more member servers within the database availability group.

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.65 EX19-MB-000236 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The application must protect the confidentiality and integrity of transmitted information.

```
GROUP ID: V-259710
RULE ID: SV-259710r961632
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised since unprotected communications can be intercepted and either read or altered.

This requirement applies only to those applications that are either distributed or can allow access to data nonlocally. Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, applications need to leverage transmission protection mechanisms, such as TLS, TLS VPNs, or IPsec.

Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-APP-000219

Audit:

Note: AuthMechanism may include other mechanisms as long as the "Tls" is identified.

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select-Object -Property Name, Identity, AuthMechanism
```

For each Receive connector, if the value of "AuthMechanism" is not set to "Tls", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -AuthMechanism 'Tls'
```

Note: The <IdentityName> value must be in quotes.

Repeat the procedures for each Receive connector.

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

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

1.66 EX19-MB-000244 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have the most current, approved Cumulative Update installed.

```
GROUP ID: V-259711
RULE ID: SV-259711r961683
```

Rationale:

Failure to install the most current Exchange Cumulative Update (CU) leaves a system vulnerable to exploitation. Current CUs correct known security and system vulnerabilities.

Audit:

Determine the most current, approved service pack.

Open the Exchange Management Shell and enter the following command:

```
Get-ExchangeServer | Select-Object -Property Name, AdminDisplayVersion
|Format-List
```

If the value of "AdminDisplayVersion" does not return the most current, approved Cumulative Update (CU), this is a finding.

Remediation:

Consult the EDSP for the accepted update process within the organization.

Install the most current, approved CU. Microsoft recommends as a best practice to always install the latest CU when creating a new server. Existing servers keep as up-to-date as possible and backup any customizations. Follow any additional recommendations by going to the following website:

https://learn.microsoft.com/en-us/Exchange/plan-and-deploy/install-cumulative-updates?view=exchserver-2019

All Exchange 2019 updates can be found on the Microsoft Exchange update site:

https://learn.microsoft.com/en-us/Exchange/new-features/updates?view=exchserver-2019

Exchange CUs must be manually downloaded. Since CUs are full installations of Exchange, there is no need to install the "Release to Manufacturer" version first. However, once installed, it cannot be uninstalled. Installation must be done on a test server first before placing in production to ensure that it does not disrupt services or conflict with existing configurations.

Note: Some CUs will require an Active Directory Schema extension, which adds new Exchange attributes. Consult the EDSP and ensure appropriate permissions before beginning an update.

Note: Security updates (SUs) can be downloaded and triggered through Windows Updates by going to Windows Update >>Advanced Options >> "Choose how updates are installed" and select the box "Give me updates for other Microsoft products when I update Windows" if the Exchange server is connected to the web or internal Windows Update Services.

Additional Information:

CCI-002605 Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c
- NIST SP 800-53 Revision 5::SI-2 c

1.67 EX19-MB-000283 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must be configured in accordance with the security configuration settings based on DOD security configuration or implementation guidance, including STIGs, NSA configuration guides, CTOs, and DTMs.

```
GROUP ID: V-259712
RULE ID: SV-259712r961863
```

Rationale:

Configuring Exchange to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DOD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the application, including the parameters required to satisfy other security control requirements.

Audit:

Open a Windows PowerShell Module and enter the following commands:

```
Get-Website | Select-Object -Property Name
Get-WebBinding -Name <'WebSiteName'> | Format-List
```

If the Web binding values returned are not on standard port 80 for HTTP connections or port 443 for HTTPS connections, this is a finding.

Note: This is excluding the Exchange Back End website which uses 81/444.

Repeat the process for each website.

Remediation:

Configure web ports to be ports 80 and 443, as specified by PPSM standards.

In an Exchange Management Shell, run the following cmdlet on the "Default Web Site":

```
Set-WebBinding -Name 'Default Web Site' -BindingInformation "127.0.0.1:443:"
-PropertyName Port -Value 443
Set-WebBinding -Name 'Default Web Site' -BindingInformation ":443:" -
PropertyName Port -Value 443
```

Note: This does not apply to the Exchange Back End website.

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	EX19-MB-000006 (Manual)	☐	☐
1.2	EX19-MB-000007 (Manual)	☐	☐
1.3	EX19-MB-000008 (Manual)	☐	☐
1.4	EX19-MB-000016 (Manual)	☐	☐
1.5	EX19-MB-000019 (Manual)	☐	☐
1.6	EX19-MB-000020 (Manual)	☐	☐
1.7	EX19-MB-000021 (Manual)	☐	☐
1.8	EX19-MB-000031 (Manual)	☐	☐
1.9	EX19-MB-000032 (Manual)	☐	☐
1.10	EX19-MB-000033 (Manual)	☐	☐
1.11	EX19-MB-000034 (Manual)	☐	☐
1.12	EX19-MB-000040 (Manual)	☐	☐
1.13	EX19-MB-000041 (Manual)	☐	☐
1.14	EX19-MB-000042 (Manual)	☐	☐
1.15	EX19-MB-000048 (Manual)	☐	☐
1.16	EX19-MB-000052 (Manual)	☐	☐
1.17	EX19-MB-000053 (Manual)	☐	☐
1.18	EX19-MB-000054 (Manual)	☐	☐
1.19	EX19-MB-000058 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	EX19-MB-000061 (Manual)	☐	☐
1.21	EX19-MB-000063 (Manual)	☐	☐
1.22	EX19-MB-000064 (Manual)	☐	☐
1.23	EX19-MB-000065 (Manual)	☐	☐
1.24	EX19-MB-000066 (Manual)	☐	☐
1.25	EX19-MB-000105 (Manual)	☐	☐
1.26	EX19-MB-000106 (Manual)	☐	☐
1.27	EX19-MB-000115 (Manual)	☐	☐
1.28	EX19-MB-000116 (Manual)	☐	☐
1.29	EX19-MB-000117 (Manual)	☐	☐
1.30	EX19-MB-000121 (Manual)	☐	☐
1.31	EX19-MB-000122 (Manual)	☐	☐
1.32	EX19-MB-000123 (Manual)	☐	☐
1.33	EX19-MB-000124 (Manual)	☐	☐
1.34	EX19-MB-000125 (Manual)	☐	☐
1.35	EX19-MB-000126 (Manual)	☐	☐
1.36	EX19-MB-000127 (Manual)	☐	☐
1.37	EX19-MB-000128 (Manual)	☐	☐
1.38	EX19-MB-000129 (Manual)	☐	☐
1.39	EX19-MB-000130 (Manual)	☐	☐
1.40	EX19-MB-000131 (Manual)	☐	☐
1.41	EX19-MB-000132 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	EX19-MB-000134 (Manual)	☐	☐
1.43	EX19-MB-000135 (Manual)	☐	☐
1.44	EX19-MB-000137 (Manual)	☐	☐
1.45	EX19-MB-000136 (Manual)	☐	☐
1.46	EX19-MB-000138 (Manual)	☐	☐
1.47	EX19-MB-000139 (Manual)	☐	☐
1.48	EX19-MB-000140 (Manual)	☐	☐
1.49	EX19-MB-000142 (Manual)	☐	☐
1.50	EX19-MB-000146 (Manual)	☐	☐
1.51	EX19-MB-000147 (Manual)	☐	☐
1.52	EX19-MB-000158 (Manual)	☐	☐
1.53	EX19-MB-000194 (Manual)	☐	☐
1.54	EX19-MB-000173 (Manual)	☐	☐
1.55	EX19-MB-000196 (Manual)	☐	☐
1.56	EX19-MB-000197 (Manual)	☐	☐
1.57	EX19-MB-000198 (Manual)	☐	☐
1.58	EX19-MB-000203 (Manual)	☐	☐
1.59	EX19-MB-000229 (Manual)	☐	☐
1.60	EX19-MB-000230 (Manual)	☐	☐
1.61	EX19-MB-000231 (Manual)	☐	☐
1.62	EX19-MB-000232 (Manual)	☐	☐
1.63	EX19-MB-000233 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	EX19-MB-000234 (Manual)	☐	☐
1.65	EX19-MB-000236 (Manual)	☐	☐
1.66	EX19-MB-000244 (Manual)	☐	☐
1.67	EX19-MB-000283 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08/14/2025	1.0.0	Initial CIS Release