CIS Microsoft Exchange 2019 Edge 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 Edge Server Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 30 Jan 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Exchange 2019 Edge 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 Edge Server

Recommendations

1 STIG RULES

Microsoft Exchange Server 2019

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

Version: 2 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 EX19-ED-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

SchUseStrongCrypto must be enabled.

```
GROUP ID: V-259577
RULE ID: SV-259577r960759
```

Rationale:

Exchange Server 2019 is configured by default with TLS 1.2. However, SchUseStrongCrypto is not set by default and must be configured to meet the TLS requirement. The strong cryptography (configured by the SchUseStrongCrypto registry value) uses more secure network protocols (TLS 1.2, TLS 1.1, and TLS 1.0) and blocks protocols that are not secure. SchUseStrongCrypto affects only client (outgoing) connections in the application.

Audit:

In a PowerShell window, run the following commands:

```
Get-ItemProperty HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319
```

If the value "SchUseStrongCrypto" is not present and set to 1, this is a finding.

Remediation:

In a PowerShell window with elevated privileges, run the following commands:

```
reg add HKLM\SOFTWARE\Microsoft\.NetFramework\v4.0.30319 /v
"SchUseStrongCrypto" /t REG_DWORD /d 1

reg add HKLM\SOFTWARE\WoW6432Node\Microsoft\.NetFramework\v4.0.30319 /v
"SchUseStrongCrypto" /t REG_DWORD /d 1
```

This will create the value within the necessary key and set the data to 1.

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-ED-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange servers must use approved DOD certificates.

```
GROUP ID: V-259578
RULE ID: SV-259578r960792
```

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-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

1.3 EX19-ED-000017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have accepted domains configured.

```
GROUP ID: V-259579
RULE ID: SV-259579r960801
```

Rationale:

Exchange may be configured to accept email for multiple domain names. This setting identifies the domains for which the server will accept mail. This check verifies the email server is not accepting email for unauthorized domains.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine the Accepted Domain values.

Open the Exchange Management Shell and enter the following command:

```
Get-AcceptedDomain | Select-Object -Property Name, DomainName, Identity,
Default
```

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

or

If the "Default" value for "AcceptedDomains" is set to another value other than "True" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP.

Open the Exchange Management Shell and enter the following command:

```
Set-AcceptedDomain -Identity <'IdentityName'> -MakeDefault $true
```

Note: The <IdentityName> 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

1.4 EX19-ED-000019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange external Receive connectors must be domain secure-enabled.

```
GROUP ID: V-259580
RULE ID: SV-259580r960840
```

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 authentication method used for communications between servers. With this feature enabled, messages can be securely passed from a partner domain securely.

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-ReceiveConnector | Select-Object -Property Name, Identity,
DomainSecureEnabled
```

For each receive connector, if the value of "DomainSecureEnabled" is not set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -DomainSecureEnabled $true
```

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

Repeat the procedures for each receive connector.

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

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

1.5 EX19-ED-000026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-259581
RULE ID: SV-259581r960879
```

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 broken up into 29 main "services", each of which has anywhere from two to 26 "categories" of events to be monitored. Moreover, each category may be set to one of four levels of logging: Lowest, Low, CAT II, and High, depending on how much detail one desires. The higher the level of detail, the more disk space required 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 deal 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 any "EventLogLevel" values returned are not set to "Lowest", this is a finding.

Note: The 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

1.6 EX19-ED-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange connectivity logging must be enabled.

```
GROUP ID: V-259582
RULE ID: SV-259582r960879
```

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 Hub Transport servers and Edge Transport servers. 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 at the Hub server, the setting will apply to both Hub and Edge 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

1.7 EX19-ED-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange queue monitoring must be configured with threshold and action.

```
GROUP ID: V-259584
RULE ID: SV-259584r960918
```

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 exist occasionally. Frequent alerts against this counter may indicate a network or other issue (such as inbound spammer traffic) that directly impacts email delivery.

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

Audit:

Note: By default, there are two user-defined data collector sets created by Exchange: ExchangeDiagnosticsDailyPerformanceLog and ExchangeDiagnosticsPerformanceLog. These are not providing enough data to monitor SMTP queues per the requirement. Additionally, if a third-party application is performing monitoring functions, the reviewer should verify the application is monitoring correctly and mark the vulnerability Not Applicable.

Open the Exchange Management Shell and enter the following command:

perfmon

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

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 Performance >> Data Collector Sets >> User Defined.

In left pane, right-click User Defined >> New >> Data Collector Set 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)

1.8 EX19-ED-000034 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange message tracking logging must be enabled.

```
GROUP ID: V-259583
RULE ID: SV-259583r960900
```

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

1.9 EX19-ED-000044 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange audit data must be protected against unauthorized access (read access).

```
GROUP ID: V-259585
RULE ID: SV-259585r960930
```

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).

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

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

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

1.10 EX19-ED-000045 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange audit data must be protected against unauthorized access for modification.

```
GROUP ID: V-259586
RULE ID: SV-259586r960933
```

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).

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

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

Remediation:

Update the EDSP to reflect the authorized groups or users that should have modify permissions to the audit data.

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

1.11 EX19-ED-000046 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange audit data must be protected against unauthorized access for deletion.

```
GROUP ID: V-259587
RULE ID: SV-259587r960936
```

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).

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

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 reflect the authorized groups or users that should have delete permissions for the audit data.

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

1.12 EX19-ED-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange audit data must be on separate partitions.

```
GROUP ID: V-259588
RULE ID: SV-259588r960948
```

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).

Determine the audit logs' assigned partition.

Note: 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.

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)

1.13 EX19-ED-000053 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange local machine policy must require signed scripts.

```
GROUP ID: V-259589
RULE ID: SV-259589r1015762
```

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)

1.14 EX19-ED-000055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must not send customer experience reports to Microsoft.

```
GROUP ID: V-259590
RULE ID: SV-259590r960963
```

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 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-OrganizationConfig | Select-Object -Property Name, Identity,
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
```

Note: This can be done during initial installation of Exchange.

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

1.15 EX19-ED-000056 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Send Fatal Errors to Microsoft must be disabled.

```
GROUP ID: V-259591
RULE ID: SV-259591r960963
```

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 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 to Microsoft must not be sent.

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 procedure for each identity.

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

1.16 EX19-ED-000094 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange queue database must reside on a dedicated partition.

```
GROUP ID: V-259592
RULE ID: SV-259592r961095
```

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:

Open the Exchange Management Shell and run the following command:

```
Get-Content $exbin\EdgeTransport.exe.config |Select-String
"QueueDatabasePath" -SimpleMatch
```

Example Output:

```
<add key="QueueDatabasePath" value="F:\Program Files\Microsoft\Exchange
Server\V15\TransportRoles\data\Queue" />
```

If the path of the Queue Database is in the same volume as the installation of Exchange, this is a finding.

If the path of the Queue Database is on the same volume of existing applications, this is a finding.

Remediation:

It is recommended to follow the instructions found in the following documentation:

https://learn.microsoft.com/en-us/exchange/mail-flow/queues/relocate-queue-database?view=exchserver-2019

Set aside time for maintenance before correcting the issue, as this will affect mail flow through the Edge role on that server.

Open an Exchange Management Shell and use the automated script (shipped with Exchange) to move the queue database and its existing files to the new destination.

The following parameters must be answered to successfully complete the move:

-queueDatabasePath #New destination for the Queue Database. If destination does not exist, the script will create it with the appropriate permissions.

-queueDatabaseLoggingPath #New destination for the Queue Database Logs. If destination does not exist, the script will create it with the appropriate permissions.

-ipFilterDatabasePath #New destination for the IP filtering Database. If the destination does not exist, the script will create it with the appropriate permissions.

-ipFilterDatabaseLoggingPath #New destination for the IP filtering Database Logs. If the destination does not exist, the script will create it with the appropriate permissions.

-temporaryStorage #This will be the path that the script moves the old version of the EdgeTransport.exe.config. The new version will have the updated path.

Note: Always back up the configuration file as CUs will overwrite any added custom configuration.

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

1.17 EX19-ED-000095 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internet-facing send connectors must specify a Smart Host.

```
GROUP ID: V-259593
RULE ID: SV-259593r961101
```

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:

Note: This is not applicable for SIPR enclaves.

Review the Email Domain Security Plan (EDSP).

Determine the internet-facing connectors.

Open the Exchange Management Shell and enter the following command:

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

For each send connector, if the value of "SmartHosts" does not return the Smart Host IP Address and the value for "DNSRoutingEnabled" is not set to "False", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

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

Note: The <IdentityName> value 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

1.18 EX19-ED-000098 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internal send connectors must use domain security (mutual authentication Transport Layer Security).

```
GROUP ID: V-259594
RULE ID: SV-259594r1043178
```

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 authentication method used for communications between servers. With this feature enabled, only servers capable of supporting domain authentication 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,
DomainSecureEnabled
```

For each send connector, if the value of "DomainSecureEnabled" is not set to "True", this is a finding.

If the "TlsAuthLevel" parameter is set to "DomainValidation" then the "TlsDomain" parameter is required if "DNSRoutingEnabled" parameter is set to "$false".

The "DNSRoutingEnabled" parameter must be "$true" If the value of "DomainSecureEnabled" is "$true".

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-SendConnector <'IdentityName'> -DomainSecureEnabled $true
```

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

Repeat the procedure for each send 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

1.19 EX19-ED-000099 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internet-facing receive connectors must offer Transport Layer Security (TLS) before using basic authentication.

```
GROUP ID: V-259595
RULE ID: SV-259595r1043178
```

Rationale:

Sending unencrypted email over the internet increases the risk that messages can be intercepted or altered. TLS is designed to protect confidentiality and data integrity by encrypting email messages between servers and thereby reducing the risk of eavesdropping, interception, and alteration. This setting forces Exchange to offer TLS before using basic authentication.

Audit:

Note: This is not applicable for SIPR enclaves.

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, BasicAuth, BasicAuthRequireTLS", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -AuthMechanism 'Tls,
BasicAuth, BasicAuthRequireTLS'
```

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

Example only for the Identity: <ServerName>\Frontend <ServerName>

Repeat the procedure 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

1.20 EX19-ED-000109 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

More than one Edge server must be deployed.

```
GROUP ID: V-259596
RULE ID: SV-259596r961152
```

Rationale:

To ensure hostile insiders are unable to easily commit DoS attacks and reduce the effectiveness of mail flow throughout the environment, a second Edge server is deployed to allow for multiple paths of mail flow both internally and externally into the environment. This prevents a single point-of-failure and allows for service to continue in the event of a DoS attack targeting one Edge role.

Audit:

Review the EDSP for current configuration.

On the mailbox server, open a PowerShell prompt and run the following command:

```
Get-EdgeSubscription
```

If there is only one subscription on each server, this is a finding.

Remediation:

At a minimum, a second server must be deployed and subscribed to.

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)

1.21 EX19-ED-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Outbound Connection Timeout must be 10 minutes or less.

```
GROUP ID: V-259597
RULE ID: SV-259597r961155
```

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.

Connections, once established, 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).

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

Remediation:

Update the EDSP to reflect the Connection Timeout 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

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

Repeat the procedure 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)

1.22 EX19-ED-000111 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Outbound Connection limit per Domain Count must be controlled.

```
GROUP ID: V-259598
RULE ID: SV-259598r961155
```

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 and works in conjunction with the Maximum Outbound Connections Count setting 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 the 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).

Determine the value for Maximum 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 the value of "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 reflect the value for Maximum Domain Connections.

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

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)

1.23 EX19-ED-000112 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange receive connector maximum hop count must be 60.

```
GROUP ID: V-259599
RULE ID: SV-259599r961155
```

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 from 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 set too high, an undeliverable message may cycle between servers, raising the risk of network congestion.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine the value for receive connectors.

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select-Object -Property Name, Identity, 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, this is not a finding.

Remediation:

Update the EDSP to reflect the value for receive connectors.

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -MaxHopCount 60
```

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

or

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)

1.24 EX19-ED-000113 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-259600
RULE ID: SV-259600r961155
```

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 connecters:

"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. IMAP Secure is not restricted and may be configured.

"Default Servername" accepts connections from other mailbox servers and any Edge Transport servers. Their default value for MaxRecipientsPerMessage is 5000.

Audit:

Review the Email Domain Security Plan (EDSP).

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, 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 reflect the Maximum Recipients per Message value.

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

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)

1.25 EX19-ED-000114 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange send connector connections count must be limited.

```
GROUP ID: V-259601
RULE ID: SV-259601r961155
```

Rationale:

This 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 the 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 the value of "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 reflect the value for SMTP Server Maximum Outbound Connections.

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

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)

1.26 EX19-ED-000115 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange message size restrictions must be controlled on Send connectors.

```
GROUP ID: V-259602
RULE ID: SV-259602r961155
```

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 EDSP.

Audit:

Review the Email Domain Security Plan (EDSP).

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 reflect the maximum message send size.

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

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

Repeat the procedure 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)

1.27 EX19-ED-000116 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange send connectors delivery retries must be controlled.

```
GROUP ID: V-259603
RULE ID: SV-259603r961155
```

Rationale:

This setting controls the rate at which delivery attempts from the home domain are retried and user notifications are issued and notes the expiration time when the message will be discarded.

If delivery retry attempts are too frequent, servers will generate network congestion. If they are too far apart, messages may remain queued longer than necessary, potentially raising disk resource requirements.

The default values of these fields should be adequate for most environments. Administrators may wish to modify the values, but changes should be documented in the System Security Plan.

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

Audit:

Review the Email Domain Security Plan (EDSP).

Determine the value for Transient Failure Retry Count.

Open the Exchange Management Shell and enter the following command:

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

If the value of "TransientFailureRetryCount" is not set to "10" or less, this is a finding.

or

If the value of "TransientFailureRetryCount" is set to more than "10" or has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to reflect the value for Transient Failure Retry Count.

Open the Exchange Management Shell and enter the following command:

```
Set-TransportService -Identity <'IdentityName'> -TransientFailureRetryCount
10
```

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

or

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)

1.28 EX19-ED-000117 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange receive connectors must be clearly named.

```
GROUP ID: V-259604
RULE ID: SV-259604r961155
```

Rationale:

For receive connectors, unclear naming as to direction and purpose increases risk that messages may not flow as intended, troubleshooting efforts may be impaired, or incorrect assumptions may be made about the completeness of the configuration.

Collectively, connectors should account for all connections required for the overall email topology design. Simple Mail Transfer Protocol (SMTP) connectors, when listed, must name purpose and direction clearly, and their counterparts on servers to which they connect should be recognizable as their partners.

Audit:

Open the Exchange Management Shell and enter the following command:

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

For each receive connector, review the naming for connectors.

If the connectors are not clearly named for purpose and direction, this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Name <'NewName'> -Identity <'IdentityName'>
```

Note: Both the <NewName> and <IdentityName> value must be in quotes.

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)

1.29 EX19-ED-000118 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange receive connectors must control the number of recipients chunked on a single message.

```
GROUP ID: V-259605
RULE ID: SV-259605r961155
```

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 enable "chunking" on received messages as they arrive at the domain. This is done so large message bodies can be relayed by the remote sender to the Receive connector in multiple, smaller chunks.

Audit:

Open the Exchange Management Shell and enter the following command:

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

For each receive connector, if the value of "ChunkingEnabled" is not set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -ChunkingEnabled $true
```

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

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)

1.30 EX19-ED-000119 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange internet receive connector connections count must be set to default.

```
GROUP ID: V-259606
RULE ID: SV-259606r961155
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. This configuration controls the maximum number of simultaneous inbound connections allowed to the SMTP server.

By default, the number of simultaneous inbound connections is 5000. If a limit is set too low, the connections pool may be filled. If attackers perceive the limit is too low, they could deny service to the Simple Mail Transfer Protocol (SMTP) server by using a connection count that exceeds the limit set. By setting the default configuration to 5000, attackers would need many more connections to cause denial of service.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine the Maximum Inbound connections value.

Open the Exchange Management Shell and enter the following command:

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

Identify internet-facing connectors.

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

or

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

Remediation:

Update the EDSP to reflect the Maximum Inbound connections value.

Open the Exchange Management Shell and enter the following command:

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

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

or

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)

1.31 EX19-ED-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Message size restrictions must be controlled on receive connectors.

```
GROUP ID: V-259607
RULE ID: SV-259607r961155
```

Rationale:

Email system availability depends in part on best practices 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 EDSP.

Audit:

Review the Email Domain Security Plan (EDSP).

Determine the global maximum message receive size.

Open the Exchange Management Shell and enter the following command:

Identify internet-facing connectors.

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

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 reflect the global maximum message receive size.

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

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)

1.32 EX19-ED-000122 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Active hyperlinks in messages from non .mil domains must be rendered unclickable.

```
GROUP ID: V-259608
RULE ID: SV-259608r961161
```

Rationale:

Active hyperlinks within an email are susceptible to attacks of malicious software or malware. The hyperlink could lead to a malware infection or redirect the website to another fraudulent website without the user's consent or knowledge.

Exchange does not have a built-in message filtering capability. DOD Enterprise Email (DEE) has created a custom resolution to filter messages from non-.mil users that have hyperlinks in the message body. The hyperlink within the messages will be modified, preventing end users from automatically clicking links.

Audit:

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.

Note: If system is on SIPRNet, this is not applicable.

Review the Email Domain Security Plan (EDSP).

Determine the name of the Transport Agent.

Open the Windows PowerShell console and enter the following command:

```
Get-TransportAgent -Name 'customAgent' | Format-List
```

If the value does not return "customAgent", this is a finding.

Note: "customAgent" is the name of the custom agent developed to render hyperlink email sources from non .mil domains as unclickable.

Remediation:

Update the EDSP to reflect the name of the Transport Agent.

Contact the DISA Enterprise Email Service Desk at disa.tinker.eis.mbx.dod-enterprise-services-service-desk@mail.mil and request the Agent and installation procedures.

or

Contact DEE Engineering PMO and request the Agent and installation procedures.

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)

1.33 EX19-ED-000123 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange messages with a blank sender field must be rejected.

```
GROUP ID: V-259609
RULE ID: SV-259609r961161
```

Rationale:

By performing filtering at the perimeter, up to 90 percent of spam, malware, and other undesirable messages are eliminated from the message stream rather than admitting them into the mail server environment. Anonymous email (messages with blank sender fields) cannot be replied to. Messages formatted in this way may be attempting to hide their true origin to avoid responses or to spam any receiver with impunity while hiding their source of origination.

Rather than spend resources and risk infection while evaluating them, it is recommended that these messages be filtered immediately upon receipt and not forwarded to end users.

Audit:

This requirement is Not Applicable for SIPR enclaves.

This requirement is Not Applicable if the organization subscribes to EEMSG or other similar DOD enterprise protections for email services.

Open the Exchange Management Shell and enter the following command:

```
Get-SenderFilterConfig | Select-Object -Property Name, Action
```

If the value of "Action" is not set to "Reject", this is a finding.

Note: "Reject" is the default value.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-SenderFilterConfig -Action Reject
```

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)

1.34 EX19-ED-000124 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange messages with a blank sender field must be filtered.

```
GROUP ID: V-259610
RULE ID: SV-259610r961161
```

Rationale:

By performing filtering at the perimeter, up to 90 percent of spam, malware, and other undesirable messages are eliminated from the message stream rather than admitting them into the mail server environment. Anonymous email (messages with blank sender fields) cannot be replied to. Messages formatted in this way may be attempting to hide their true origin to avoid responses or to spam any receiver with impunity while hiding their source of origination.

Rather than spend resources and risk infection while evaluating them, it is recommended that these messages be filtered immediately upon receipt and not forwarded to end users.

Audit:

This requirement is Not Applicable for SIPR enclaves.

This requirement is Not Applicable if the organization subscribes to EEMSG or other similar DOD enterprise protections for email services.

Open the Exchange Management Shell and enter the following command:

```
Get-SenderFilterConfig | Select-Object -Property Name,
BlankSenderBlockingEnabled
```

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

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-SenderFilterConfig -BlankSenderBlockingEnabled $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)

1.35 EX19-ED-000125 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange filtered messages must be archived.

```
GROUP ID: V-259611
RULE ID: SV-259611r961161
```

Rationale:

By performing filtering at the perimeter, up to 90 percent of spam, malware, and other undesirable messages are eliminated from the message stream rather than admitting them into the mail server environment. This significantly reduces the attack vector for inbound email-borne spam and malware.

As messages are filtered, it is prudent to temporarily host them in an archive for evaluation by administrators or users. The archive can be used to recover messages that might have been inappropriately filtered, preventing data loss, and to provide a base of analysis that can provide future filter refinements.

Audit:

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement.

Open the Exchange Management Shell and enter the following command:

```
Get-ContentFilterConfig | Select-Object -Property Name, quarantineMailbox
```

If no SMTP address is assigned to "quarantineMailbox", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ContentFilterConfig -quarantineMailbox <'quarantineMailbox SmtpAddress'>
```

Note: The <quarantineMailbox SmtpAddress> 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)

1.36 EX19-ED-000126 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange sender filter must block unaccepted domains.

```
GROUP ID: V-259612
RULE ID: SV-259612r961161
```

Rationale:

Spam origination sites and other sources of suspected email-borne malware have the ability to corrupt, compromise, or otherwise limit availability of email servers. Limiting exposure to unfiltered inbound messages can reduce the risk of spam and malware impacts.

The Global Deny list blocks messages originating from specific sources. Most block list filtering is done using a commercial block list service, because eliminating threats from known spammers prevents the messages being evaluated inside the enclave where there is more risk they can do harm.

Additional sources should also be blocked to supplement the contents of the commercial Block List service. For example, during a zero-day threat action, entries can be added and then removed when the threat is mitigated. An additional best practice is to enter the enterprise's home domains in the block list, because inbound email with a "from" address of the home domain is very likely to be spoofed spam.

Audit:

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement.

Review the Email Domain Security Plan (EDSP).

Determine the unaccepted domains that are to be blocked.

Open the Exchange Management Shell and enter the following command:

```
Get-SenderFilterConfig | Select-Object -Property Name, BlockedDomains,
BlockedDomainsAndSubdomains
```

If the value for "BlockedDomains" or "BlockedDomainsAndSubdomains" does not reflect the list of accepted domains, this is a finding.

Remediation:

Update the EDSP to reflect the unaccepted domains that are to be blocked.

Open the Exchange Management Shell and enter the following command:

For BlockedDomains:

```
Set-SenderFilterConfig -BlockedDomains <BlockedDomain>
```

To add additional domains to the list (array):

```
Set-SenderFilterConfig -BlockedDomains
@{add="<blockeddomain2>","<blockeddomain3>","<blockeddomain4>"}
```

Each domain added must be quotes and separated by a comma.

Repeat the procedure for each domain that is to be blocked.

or

For BlockedDomainsAndSubdomains:

```
Set-SenderFilterConfig -BlockedDomainsAndSubdomains
<BlockedDomainAndSubdomain>
```

Same procedure applies for adding multiple domains applies to this filter.

Repeat the procedure for each domain and all of its subdomains that are to be blocked.

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)

1.37 EX19-ED-000127 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange nonexistent recipients must not be blocked.

```
GROUP ID: V-259613
RULE ID: SV-259613r961161
```

Rationale:

Spam originators, in an effort to refine mailing lists, sometimes use a technique where they first create fictitious names and then monitor rejected emails for nonexistent recipients. Those not rejected are deemed to exist and are used in future spam mailings.

To prevent this disclosure of existing email accounts to spammers, email to nonexistent recipients must not be blocked. Instead, it is recommended that all messages be received, then evaluated and disposed of without enabling the sender to determine existent versus nonexistent recipients.

Audit:

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement.

Additionally, the default value for "RecipientValidationEnabled" is "False".

Open the Exchange Management Shell and enter the following command:

```
Get-RecipientFilterConfig | Select-Object -Property Name,
RecipientValidationEnabled
```

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

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-RecipientFilterConfig -RecipientValidationEnabled $false
```

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)

1.38 EX19-ED-000128 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Sender Reputation filter must be enabled.

```
GROUP ID: V-259614
RULE ID: SV-259614r961161
```

Rationale:

By performing filtering at the perimeter, up to 90 percent of spam, malware, and other undesirable messages are eliminated from the message stream rather than admitting them into the mail server environment. Sender Reputation is anti-spam functionality that blocks messages according to many characteristics of the sender. Sender Reputation relies on persisted data about the sender to determine what action, if any, to take on an inbound message. This setting enables the Sender Reputation function.

Audit:

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement.

Additionally, the default value for "Sender Reputation" is "True" for "Enabled".

Open the Exchange Management Shell and enter the following command:

```
Get-SenderReputationConfig | Select-Object -Property Name, Enabled
```

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

Remediation:

Open the Exchange Management Shell and enter the following command:

```
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)

1.39 EX19-ED-000129 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Sender Reputation filter must identify the spam block level.

```
GROUP ID: V-259615
RULE ID: SV-259615r961161
```

Rationale:

By performing filtering at the perimeter, up to 90 percent of spam, malware, and other undesirable messages are eliminated from the message stream rather than admitting them into the mail server environment. Sender Reputation is anti-spam functionality that blocks messages according to many characteristics of the sender. Sender Reputation relies on persisted data about the sender to determine what action, if any, to take on an inbound message. This setting enables the threshold at which an email will be considered spam.

Audit:

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement.

Review the Email Domain Security Plan (EDSP).

Determine the SrlBlockThreshold value.

Open the Exchange Management Shell and enter the following command:

```
Get-SenderReputationConfig | Select-Object -Property Name, SrlBlockThreshold
```

If the value of SrlBlockThreshold is not set to "6", this is a finding.

or

If the value of "SrlBlockThreshold" is set to a value other than "6" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to reflect the SrlBlockThreshold size.

Open the Exchange Management Shell and enter the following command:

```
Set-SenderReputationConfig -SrlBlockThreshold 6
```

or

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

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)

1.40 EX19-ED-000131 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Spam Evaluation filter must be enabled.

```
GROUP ID: V-259617
RULE ID: SV-259617r961161
```

Rationale:

By performing filtering at the perimeter, up to 90 percent of spam, malware, and other undesirable messages may be eliminated from the transport message stream, preventing their entry into the Exchange environment. This significantly reduces the attack vector for inbound email-borne spam and malware.

Spam Evaluation filters scan inbound email messages for evidence of spam and other attacks that primarily use social engineering techniques. Upon evaluation completion, a rating is assigned to each message estimating the likelihood of its being spam. Upon arrival at the destination mailbox, the junk mail filter threshold (also configurable) determines whether the message will be withheld from delivery, delivered to the junk mail folder, or delivered to the user's inbox.

Audit:

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement. Additionally, the default value for this property is Enabled "True".

Open the Exchange Management Shell and enter the following command:

```
Get-ContentFilterConfig | Select-Object -Property Name, Identity, Enabled
```

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

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ContentFilterConfig -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)

1.41 EX19-ED-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Attachment filtering must remove undesirable attachments by file type.

```
GROUP ID: V-259616
RULE ID: SV-259616r961161
```

Rationale:

By performing filtering at the perimeter, up to 90 percent of spam, malware, and other undesirable messages are eliminated from the message stream rather than admitting them into the mail server environment.

Attachments are being used more frequently for different forms of attacks. By filtering undesirable attachments, a large percent of malicious code can be prevented from entering the system. Attachments must be controlled at the entry point into the email environment to prevent successful attachment-based attacks. The following is a basic list of known attachments that should be filtered from internet mail attachments:

*.ade *.crt *.jse *.msi *.scr *.wsh *.dir *.adp *.csh *.ksh *.msp *.sct *.htm *.dcr *.app *.exe *.lnk *.mst *.shb *.html *.plg *.asx *.fxp *.mda *.ops *.shs *.htc *.spl *.bas *.hlp *.mdb *.pcd *.url *.mht *.swf *.bat *.hta *.mde *.pif *.vb *.mhtml *.zip *.chm *.inf *.mdt *.prf *.vbe *.shtm *.cmd *.ins *.mdw *.prg *.vbs *.shtml *.com *.isp *.mdz *.reg *.wsc *.stm *.cpl *.js *.msc *.scf *.wsf *.xml

Audit:

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement.

Review the Email Domain Security Plan (EDSP).

Determine the list of undesirable attachment types that should be stripped.

Open the Exchange Management Shell and enter the following command:

```
Get-AttachmentFilterEntry
```

For each attachment type, if the values returned are different from the EDSP documented attachment types, this is a finding.

Remediation:

Update the EDSP to reflect the list of undesirable attachment types that should be stripped.

Open the Exchange Management Shell and enter the following command:

```
Add-AttachmentFilterEntry -Name <'*.FileExtension'> -Type FileName
```

Repeat the procedure for each undesirable attachment type.

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)

1.42 EX19-ED-000132 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Block List service provider must be identified.

```
GROUP ID: V-259618
RULE ID: SV-259618r961161
```

Rationale:

Block List filtering is a sanitization process performed on email messages prior to their arrival at the destination mailbox. By performing this process at the email perimeter, threats can be eliminated outside the enclave, where there is less risk for them to do harm.

Block List services (sometimes called Reputation Data services) are fee-based data providers that collect the IP addresses of known spammers and other malware purveyors. Block List service subscribers benefit from more effective spam elimination. (Spam is estimated to compose up to 90 percent of inbound mail volume.) Failure to specify a Block List provider risks that manual email administration effort would be needed to maintain and update larger Block Lists than a single email site administrator could conveniently or accurately maintain.

The Block List service vendor provides a value for this field, usually the Domain Name System (DNS) suffix for its domain.

Audit:

If not using a service provider, this requirement is not applicable.

Review the Email Domain Security Plan (EDSP).

Determine the name and information for the Block List provider.

Open the Exchange Management Shell and enter the following command:

```
Get-IPBlockListProvider | Select-Object -Property Name, Identity,
LookupDomain
```

If the values for "Name", GUID, and "LookupDomain" are not configured, this is a finding.

Remediation:

Update the EDSP to reflect the name and information for the Block List provider.

Open the Exchange Management Shell and enter the following command:

```
Set-IPBlockListProvider -Name <Provider Name> [Additional optional parameters
as required by the service provider]
```

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-ED-000133 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange messages with a malformed From address must be rejected.

```
GROUP ID: V-259619
RULE ID: SV-259619r1040909
```

Rationale:

Sender Identification (SID) is an email anti-spam sanitization process. Sender ID uses DNS MX record lookups to verify the Simple Mail Transfer Protocol (SMTP) sending server is authorized to send email for the originating domain.

Failure to implement Sender ID risks that spam could be admitted into the email domain that originates from rogue servers. Most spam content originates from domains where the IP address has been spoofed prior to sending, thereby avoiding detection. For example, messages with malformed or incorrect "purported responsible sender" data in the message header could be (best case) created by using RFI noncompliant software but is more likely to be spam.

Audit:

If this server is in a SIPR Enclave, this requirement is Not Applicable.

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement.

Open the Exchange Management Shell and enter the following command:

```
Get-SenderIdConfig | Select-Object -Property Name, Identity,
SpoofedDomainAction
```

If the value of "SpoofedDomainAction" is not set to "Reject", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-SenderIdConfig -SpoofedDomainAction Reject
```

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-ED-000134 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Recipient filter must be enabled.

```
GROUP ID: V-259620
RULE ID: SV-259620r961161
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. Careful tuning reduces the risk that system or network congestion will contribute to availability impacts.

Filters that govern inbound email evaluation can significantly reduce spam, phishing, and spoofed emails. Messages from blank senders, known spammers, or zero-day attack modifications must be enabled to be effective.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-RecipientFilterConfig | Select-Object -Property Name, Enabled
```

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

Note: The default value is set to "True".

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-RecipientFilterConfig -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)

1.45 EX19-ED-000135 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange tarpitting interval must be set.

```
GROUP ID: V-259621
RULE ID: SV-259621r961161
```

Rationale:

Tarpitting is the practice of artificially delaying server responses for specific Simple Mail Transfer Protocol (SMTP) communication patterns that indicate high volumes of spam or other unwelcome messages. The intent of tarpitting is to slow down the communication process for spam batches to reduce the cost effectiveness of sending spam and thwart directory harvest attacks.

A directory harvest attack is an attempt to collect valid email addresses from a particular organization so the email addresses can be added to a spam database. A program can be written to collect email addresses that return a "Recipient OK" SMTP response and discard all email addresses that return a "User unknown" SMTP response.

Tarpitting makes directory harvest attacks too costly to automate efficiently.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-ReceiveConnector | Select Name, Identity, TarpitInterval
```

For each Receive connector, if the value of "TarpitInterval" is not set to "00:00:05" or greater, this is a finding.

Note: The default value for "TarpitInterval" is "00:00:05".

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -TarpitInterval '00:00:05'
```

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

Repeat the procedures for each Receive connector.

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-ED-000136 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internal Receive connectors must not allow anonymous connections.

```
GROUP ID: V-259622
RULE ID: SV-259622r961161
```

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, relay hijacking 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 noninternet connector, this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -PermissionGroups 'valid user group(s)'
```

Note: The <IdentityName> value and user group(s) must be in quotes.

Example for user groups only: 'ExchangeServers, ExchangeUsers'

Repeat the procedures for each Receive connector.

This is an example only: Set-ReceiveConnector -Identity <'IdentityName'> -PermissionGroups 'ExchangeUsers'

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-ED-000137 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Simple Mail Transfer Protocol (SMTP) IP Allow List entries must be empty.

```
GROUP ID: V-259623
RULE ID: SV-259623r961161
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. Careful tuning reduces the risk that system or network congestion will contribute to availability impacts.

Filters that govern inbound email evaluation can significantly reduce spam, phishing, and spoofed emails. Filters for messages from blank senders, known spammers, or zero-day attack modifications must be enabled to be effective.

Having items identified in the Allow List causes other spam evaluation steps to be bypassed and therefore should be used only with an abundance of caution. If spammers were to learn of entries in the Allow List, it could enable them to plan a denial of service attack (or other attack) by spoofing that source.

Audit:

Review the Email Domain Security Plan (EDSP).

Identify the SMTP Allow List settings.

Open the Exchange Management Shell and enter the following command:

```
Get-IPAllowListEntry | Format-List
```

If the result returns any values, this is a finding.

or

If the result returns any values but has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP to reflect the SMTP Allow List settings.

Open the Exchange Management Shell and enter the following command:

Note: Remove any value(s) that are not identified by the EDSP or have not obtained a signoff with risk acceptance.

```
Remove-IPAllowListEntry -Identity <IP Allow List entry ID>
```

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-ED-000138 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Simple Mail Transfer Protocol (SMTP) IP Allow List Connection filter must be enabled.

```
GROUP ID: V-259624
RULE ID: SV-259624r961161
```

Rationale:

Email system availability depends in part on best practice strategies for setting tuning configurations. Careful tuning reduces the risk that system or network congestion will contribute to availability impacts.

Filters that govern inbound email evaluation can significantly reduce spam, phishing, and spoofed emails. Filters for messages from blank senders, known spammers, or zero-day attack modifications must be enabled to be effective.

Having items identified in the Allow List causes other spam evaluation steps to be bypassed and therefore should be used only with an abundance of caution. If spammers were to learn of entries in the Allow List, it could enable them to plan a denial of service attack (or other attack) by spoofing that source.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-IPAllowListConfig | Select-Object -Property Name, Enabled
```

If the value for "Enabled" is not set to "True", this is a finding.

Note: "Enabled" set to "True" is the default value.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-IPAllowListConfig -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)

1.49 EX19-ED-000139 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Simple Mail Transfer Protocol (SMTP) Sender filter must be enabled.

```
GROUP ID: V-259625
RULE ID: SV-259625r961161
```

Rationale:

Email system availability depends in part on best practices strategies for setting tuning configurations. Careful tuning reduces the risk that system or network congestion will contribute to availability impacts.

Filters that govern inbound email evaluation can significantly reduce spam, phishing, and spoofed emails. Filters for messages from blank senders, known spammers, or zero-day attack modifications must be enabled to be effective.

Failure to enable the filter will result in no action taken. This setting should always be enabled.

Audit:

This requirement is not applicable for SIPR enclaves.

This requirement is not applicable if the organization subscribes to EEMSG or other similar DOD enterprise protections for email services.

Open the Exchange Management Shell and enter the following command:

```
Get-SenderFilterConfig | Select-Object -Property Name, Enabled
```

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

Note: "Enabled" set to "True" is the default value.

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-SenderFilterConfig -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)

1.50 EX19-ED-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have anti-spam filtering installed.

```
GROUP ID: V-259626
RULE ID: SV-259626r961161
```

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. 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) for an installed anti-spam product.

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 | Format-Table Name, Enabled
```

If no value is returned, this is a finding.

Remediation:

Install the anti-Spam module.

Open the Exchange Management Shell and enter the following command:

```
& $env:ExchangeInstallPath\Scripts\Install-anti-SpamAgents.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)

1.51 EX19-ED-000141 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have anti-spam filtering enabled.

```
GROUP ID: V-259627
RULE ID: SV-259627r961161
```

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. 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) for an installed anti-spam product.

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 | Format-Table Name, Enabled; Get-SenderFilterConfig
| Format-Table Name, Enabled; Get-SenderIDConfig | Format-Table Name,
Enabled; Get-SenderReputationConfig | Format-Table Name, Enabled
```

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

- Set-ContentFilterConfig
- Set-SenderFilterConfig
- Set-SenderIDConfig
- Set-SenderReputationConfig

Remediation:

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)

1.52 EX19-ED-000142 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have anti-spam filtering configured.

```
GROUP ID: V-259628
RULE ID: SV-259628r961161
```

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:

The site should use an approved DOD scanner as Exchange Malware software has a limited scanning capability.

If an approved DOD scanner is not being used, this is a finding.

Remediation:

Following vendor best practice guidance, install and configure a DOD approved scanner.

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)

1.53 EX19-ED-000143 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Sender Identification Framework must be enabled.

```
GROUP ID: V-259629
RULE ID: SV-259629r961161
```

Rationale:

Email is only as secure as the recipient. When the recipient is an email server accepting inbound messages, authenticating the sender enables the receiver to better assess message quality and to validate the sending domain as authentic. One or more authentication techniques used in combination can be effective in reducing spam, phishing, and forger attacks.

The Sender ID Framework (SIDF) receiver accesses specially formatted DNS records (SPF format) that contain the IP address of authorized sending servers for the sending domain that can be compared to data in the email message header. Receivers are able to validate the authenticity of the sending domain, helping to avoid receiving inbound messages from phishing or other spam domains.

Audit:

Note: If third-party anti-spam product is being used, the anti-spam product must be configured to meet the requirement.

Open the Exchange Management Shell and enter the following command:

```
Get-SenderIdConfig | Select-Object -Property Name, Identity, Enabled
```

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

Note: By Default, the value of "Enabled" is set to "True".

Remediation:

Open the Exchange Management Shell and enter the following command:

```
Set-SenderIdConfig -Enable $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)

1.54 EX19-ED-000159 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must limit the Receive connector timeout.

```
GROUP ID: V-259630
RULE ID: SV-259630r1043182
```

Rationale:

Email system availability depends in part on best practices 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.

Audit:

Review the Email Domain Security Plan (EDSP), or Organizations applicable documentation.

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 "00:05:00", this is a finding.

If "ConnectionTimeout" is set to another value other than "00:05:00" and has signoff and risk acceptance in the EDSP, this is not a finding.

Remediation:

Update the EDSP, or the applicable documentation.

Open the Exchange Management Shell and enter the following command:

```
Set-ReceiveConnector -Identity <'IdentityName'> -ConnectionTimeout 00:05:00
```

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

or

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

Repeat the procedures for each Receive connector.

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

1.55 EX19-ED-000174 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-259631
RULE ID: SV-259631r961353
```

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 in 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:

Check the EDSP to verify who 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 who 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.

Reference 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)

1.56 EX19-ED-000195 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange application directory must be protected from unauthorized access.

```
GROUP ID: V-259632
RULE ID: SV-259632r1015763
```

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).

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

Determine if the access permissions on the directory match the access permissions listed in the EDSP.

If any group or user has different access permissions than listed in the EDSP, this is a finding.

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

Remediation:

Update the EDSP to reflect the authorized groups and users that have access to the Exchange application directories.

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)

1.57 EX19-ED-000197 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange software baseline copy must exist.

```
GROUP ID: V-259633
RULE ID: SV-259633r961461
```

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).

Determine the baseline documentation.

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:

Implement an email software baseline process and update the EDSP.

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)

1.58 EX19-ED-000198 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange local machine policy must require signed scripts.

```
GROUP ID: V-259634
RULE ID: SV-259634r1015764
```

Rationale:

Scripts, especially those downloaded from untrusted locations, often provide a way for attackers to infiltrate a system. By setting machine policy to prevent unauthorized script executions, unanticipated system impacts can be avoided.

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-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)

1.59 EX19-ED-000199 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-259635
RULE ID: SV-259635r961470
```

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 POP3 and IMAP4 clients are not included in the standard desktop offering, they must be disabled.

Audit:

Review the Email Domain Security Plan (EDSP).

Note: Required services will vary between organizations and will vary depending on the role of the individual system. Organizations will develop their own list of services, which will be documented and justified with the 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 or undocumented or unnecessary services are running, this is a finding.

Remediation:

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

Navigate to Administrator Tools >> Services and disable or remove any services that are not required.

or

in PowerShell:

Stop-Service -Name ;

Set-Service -Name -StartupType Disabled

Stop and disable 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)

1.60 EX19-ED-000224 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Edge server must point to a trusted list of DNS servers for external and internal resolution.

```
GROUP ID: V-259636
RULE ID: SV-259636r961587
```

Rationale:

To mitigate the risk of possible erroneous queries that may have been coopted by bad actors, the Exchange Edge server must use DNS servers that utilize DNSSEC to resolve external hosts and internal hosts before routing messages to the appropriate destination.

Audit:

Verify in the EDSP or consult with the appropriate personnel who manage DNS which servers to use for Internal and External DNS resolution.

If the server is not multi-homed, this does not apply.

In Exchange Management Shell, run the following command:

```
Get-TransportService |Format-List *dns*
```

If "ExternalDNSAdapterEnabled : True", and no GUID exists, this is a finding.

If "ExternalDNSAdapterEnabled : False", and the property "ExternalDNSServers" is not populated with the documented trusted DNS servers for External DNS queries, this is a finding.

If "InternalDNSAdapterEnabled : True" and no GUID exists, this is a finding.

If "InternalDNSAdapterEnabled : False" and the property "InternalDNSServers" is not populated the documented trusted DNS servers for Internal DNS queries, this is a finding.

Remediation:

Verify in the EDSP or consult with the appropriate personnel who manage which DNS servers to use for Internal and External DNS resolution.

If a GUID for the External and Internal network adapters are applicable, then gather the values to populate the appropriate properties with the following commands:

```
netsh lan show interfaces
```

This will provide the adapters and the GUIDs for each. Identify the external and internal adapters for the Edge server.

Once gathered, run the following:

```
Set-TransportService -Identity <name of server> -ExternalDNSAdapterEnabled
$true -ExternalDNSAdapterGuid <externalAdapterGUID> -
InternalDNSAdapterEnabled $true -InternalDNSAdapterGuid <InternalAdapterGuid>
```

If the "ExternalDNSAdapterEnabled" or InternalDNSAdapterEnabled are set to false, use the following to set the DNS configuration:

```
Set-TransportService -Identity  <name of server> -InternalDNSServers
@{add="Trusted DNS IP1","Trusted DNS IP2"}
Set-TransportService -Identity  <name of server> -ExternalDNSServers
@{add="Trusted DNS IP1","Trusted DNS IP2"}
```

Additional Information:

CCI-002466 Request data integrity verification on the name/address resolution responses the system receives from authoritative sources.

- NIST SP 800-53 Revision 4::SC-21
- NIST SP 800-53 Revision 5::SC-21

1.61 EX19-ED-000231 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-259638
RULE ID: SV-259638r961620
```

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 about 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
```

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.

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-ED-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange software must be installed on a separate partition from the OS.

```
GROUP ID: V-259637
RULE ID: SV-259637r961608
```

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 the directory where Exchange is installed.

Open Windows Explorer.

Navigate to the location where Exchange is installed.

If Exchange resides on a directory or partition other than that of the OS and does not have other applications installed (without associated approval from the ISSO), this is not a finding.

Remediation:

Update the EDSP to reflect the directory where Exchange is installed.

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

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

1.63 EX19-ED-000232 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internal Send connectors must use an authentication level.

```
GROUP ID: V-259639
RULE ID: SV-259639r961620
```

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
```

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
```

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-ED-000234 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Exchange must provide redundancy.

```
GROUP ID: V-259640
RULE ID: SV-259640r961632
```

Rationale:

Denial of Service (DoS) is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of applications to mitigate the impact of DoS attacks that have occurred or are ongoing on application availability. For each application, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or restricting the number of sessions the application opens at one time). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Audit:

Review the Email Domain Security Plan (EDSP).

From a Mailbox server in the subscribed Edge Subscription site, determine if the Exchange servers are using redundancy by entering the following command:

```
Get-EdgeSubscription
```

If the value returned is not at least two Edge servers, this is a finding.

Remediation:

Update the EDSP to reflect the Exchange servers used for redundancy.

Configure and subscribe to two or more Edge servers for load balancing.

Additional Information:

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

1.65 EX19-ED-000235 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Exchange internal Receive connectors must require encryption.

```
GROUP ID: V-259641
RULE ID: SV-259641r961632
```

Rationale:

The Simple Mail Transfer Protocol (SMTP) Receive connector is used by Exchange to send and receive messages from server to server using SMTP protocol. This setting controls the encryption strength used for client connections to the SMTP Receive connector. With this feature enabled, only clients capable of supporting secure communications will be able to send mail using this SMTP server. Where secure channels are required, encryption can also be selected.

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 the client to the server adds protection by encrypting the sender and recipient information that cannot be encrypted by the sender.

Individually, channel security and encryption have been 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 the client and server.

Audit:

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 process for each Receive connector.

Additional Information:

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-ED-000236 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Exchange internal Send connectors must require encryption.

```
GROUP ID: V-259642
RULE ID: SV-259642r961632
```

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:

Check the Email Domain Security Plan (EDSP) and determine which send connector is using which secure validation method. If no configuration setting is found, this is a finding.

If using "DomainValidation", open the Exchange Management Shell and enter the following command:

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

If the value of "TlsDomain" is not set to the value of the internal <'SMTP Domain'>, this is a finding.

If using "DomainSecureEnabled", open the Exchange Management Shell and enter the following command:

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

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

Note: The wildcard character (*) is not supported in domains that are configured for mutual TLS authentication. The same domain must also be defined on the corresponding Receive connector and in the TLSReceiveDomainSecureList attribute of the transport configuration.

Remediation:

If using "DomainValidation", open the Exchange Management Shell and enter the following command:

```
Set-SendConnector -Identity <'Identity'> -TlsDomain <InternalSMTPDomain> -
TlsAuthLevel DomainValidation -RequireTLS $true
```

If using "DomainSecureEnabled", open the Exchange Management Shell and enter the following command:

```
Set-SendConnector -Identity <'ReceiveConnector'> -DomainSecureEnabled $true
```

Note:

- To use DomainSecureEnabled, DNSRouting must be set to $true.
- The same domain must also be defined on the corresponding Receive connector and in the TLSReceiveDomainSecureList attribute of the transport configuration.

Additional Information:

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

1.67 EX19-ED-000238 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must render hyperlinks from email sources from non-.mil domains as unclickable.

```
GROUP ID: V-259643
RULE ID: SV-259643r961638
```

Rationale:

Active hyperlinks within an email are susceptible to attacks of malicious software or malware. The hyperlink could lead to a malware infection or redirect the website to another fraudulent website without the user's consent or knowledge.

Exchange does not have a built-in message filtering capability. DOD Enterprise Email (DEE) has created a custom resolution to filter messages from non-.mil users that have hyperlinks in the message body. The hyperlink within the messages will be modified, preventing end users from automatically clicking links.

Audit:

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.

Note: If system is on SIPRNet, this is not applicable.

Review the Email Domain Security Plan (EDSP).

Determine the name of the Transport Agent.

Open the Windows PowerShell console and enter the following command:

```
Get-TransportAgent -Name 'customAgent' | Format-List
```

If the value does not return "customAgent", this is a finding.

Note: "customAgent" is the name of the custom agent developed to render hyperlink email sources from non .mil domains as unclickable.

Remediation:

Update the EDSP to reflect the name of the Transport Agent.

Contact the DISA Enterprise Email Service Desk at disa.tinker.eis.mbx.dod-enterprise-services-service-desk@mail.mil and request the Agent and installation procedures.

or

Contact DEE Engineering PMO and request the Agent and installation procedures.

Additional Information:

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

1.68 EX19-ED-000244 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-259644
RULE ID: SV-259644r961683
```

Rationale:

The organization (including any contractor to the organization) must promptly install security-relevant software updates (e.g., patches, service packs, CUs, hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed.

Audit:

Open the Exchange Management Shell and enter the following command:

```
Get-ExchangeServer | Format-List Name, AdminDisplayVersion
```

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

Remediation:

Install the most current, approved CU.

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	EX19-ED-000006 (Manual)	☐	☐
1.2	EX19-ED-000016 (Manual)	☐	☐
1.3	EX19-ED-000017 (Manual)	☐	☐
1.4	EX19-ED-000019 (Manual)	☐	☐
1.5	EX19-ED-000026 (Manual)	☐	☐
1.6	EX19-ED-000027 (Manual)	☐	☐
1.7	EX19-ED-000040 (Manual)	☐	☐
1.8	EX19-ED-000034 (Manual)	☐	☐
1.9	EX19-ED-000044 (Manual)	☐	☐
1.10	EX19-ED-000045 (Manual)	☐	☐
1.11	EX19-ED-000046 (Manual)	☐	☐
1.12	EX19-ED-000050 (Manual)	☐	☐
1.13	EX19-ED-000053 (Manual)	☐	☐
1.14	EX19-ED-000055 (Manual)	☐	☐
1.15	EX19-ED-000056 (Manual)	☐	☐
1.16	EX19-ED-000094 (Manual)	☐	☐
1.17	EX19-ED-000095 (Manual)	☐	☐
1.18	EX19-ED-000098 (Manual)	☐	☐
1.19	EX19-ED-000099 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	EX19-ED-000109 (Manual)	☐	☐
1.21	EX19-ED-000110 (Manual)	☐	☐
1.22	EX19-ED-000111 (Manual)	☐	☐
1.23	EX19-ED-000112 (Manual)	☐	☐
1.24	EX19-ED-000113 (Manual)	☐	☐
1.25	EX19-ED-000114 (Manual)	☐	☐
1.26	EX19-ED-000115 (Manual)	☐	☐
1.27	EX19-ED-000116 (Manual)	☐	☐
1.28	EX19-ED-000117 (Manual)	☐	☐
1.29	EX19-ED-000118 (Manual)	☐	☐
1.30	EX19-ED-000119 (Manual)	☐	☐
1.31	EX19-ED-000120 (Manual)	☐	☐
1.32	EX19-ED-000122 (Manual)	☐	☐
1.33	EX19-ED-000123 (Manual)	☐	☐
1.34	EX19-ED-000124 (Manual)	☐	☐
1.35	EX19-ED-000125 (Manual)	☐	☐
1.36	EX19-ED-000126 (Manual)	☐	☐
1.37	EX19-ED-000127 (Manual)	☐	☐
1.38	EX19-ED-000128 (Manual)	☐	☐
1.39	EX19-ED-000129 (Manual)	☐	☐
1.40	EX19-ED-000131 (Manual)	☐	☐
1.41	EX19-ED-000130 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	EX19-ED-000132 (Manual)	☐	☐
1.43	EX19-ED-000133 (Manual)	☐	☐
1.44	EX19-ED-000134 (Manual)	☐	☐
1.45	EX19-ED-000135 (Manual)	☐	☐
1.46	EX19-ED-000136 (Manual)	☐	☐
1.47	EX19-ED-000137 (Manual)	☐	☐
1.48	EX19-ED-000138 (Manual)	☐	☐
1.49	EX19-ED-000139 (Manual)	☐	☐
1.50	EX19-ED-000140 (Manual)	☐	☐
1.51	EX19-ED-000141 (Manual)	☐	☐
1.52	EX19-ED-000142 (Manual)	☐	☐
1.53	EX19-ED-000143 (Manual)	☐	☐
1.54	EX19-ED-000159 (Manual)	☐	☐
1.55	EX19-ED-000174 (Manual)	☐	☐
1.56	EX19-ED-000195 (Manual)	☐	☐
1.57	EX19-ED-000197 (Manual)	☐	☐
1.58	EX19-ED-000198 (Manual)	☐	☐
1.59	EX19-ED-000199 (Manual)	☐	☐
1.60	EX19-ED-000224 (Manual)	☐	☐
1.61	EX19-ED-000231 (Manual)	☐	☐
1.62	EX19-ED-000230 (Manual)	☐	☐
1.63	EX19-ED-000232 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	EX19-ED-000234 (Manual)	☐	☐
1.65	EX19-ED-000235 (Manual)	☐	☐
1.66	EX19-ED-000236 (Manual)	☐	☐
1.67	EX19-ED-000238 (Manual)	☐	☐
1.68	EX19-ED-000244 (Manual)	☐	☐

Appendix: Change History

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