CIS Microsoft Exchange 2016 Edge Transport Server STIG Benchmark

v1.0.0 – 01-30-2025

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 2016 Edge Transport Server Secure Technical Implementation Guide (STIG)
Version: 2 Release: 6 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 2016 Edge Transport 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 2016 Edge Transport Server

Recommendations

1 STIG RULES

Microsoft Exchange 2016 Edge Transport Server

Microsoft Exchange 2016 Edge Transport Server Secure Technical Implementation Guide (STIG)

Version: 2 Release: 6 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 EX16-ED-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must limit the Receive connector timeout.

```
GROUP ID: V-221202
RULE ID: SV-221202r960735
```

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.

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

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 Name, Identity, ConnectionTimeout
For each Receive connector, if the value of "ConnectionTimeout" is not set to "00:05:00", this is a finding.
or
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 single 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-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.2 EX16-ED-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange servers must use approved DoD certificates.

```
GROUP ID: V-221203
RULE ID: SV-221203r960792
```

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 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 EX16-ED-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have accepted domains configured.

```
GROUP ID: V-221204
RULE ID: SV-221204r960801
```

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 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 single 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 EX16-ED-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange external Receive connectors must be domain secure-enabled.

```
GROUP ID: V-221206
RULE ID: SV-221206r960801
```

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 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 single quotes.
Repeat the procedures for each receive connector.

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

1.5 EX16-ED-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221207
RULE ID: SV-221207r960879
```

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 2 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.

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 single 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 EX16-ED-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Connectivity logging must be enabled.

```
GROUP ID: V-221208
RULE ID: SV-221208r960879
```

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 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 single 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 EX16-ED-000080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Queue monitoring must be configured with threshold and action.

```
GROUP ID: V-221209
RULE ID: SV-221209r960918
```

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: If a third-party application is performing monitoring functions, the reviewer should verify the application is monitoring correctly and mark the vulnerability NA.
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 on 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 EX16-ED-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must not send Customer Experience reports to Microsoft.

```
GROUP ID: V-221210
RULE ID: SV-221210r960963
```

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 non-essential 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 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

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

1.9 EX16-ED-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221211
RULE ID: SV-221211r960930
```

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 EX16-ED-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Send Fatal Errors to Microsoft must be disabled.

```
GROUP ID: V-221212
RULE ID: SV-221212r960963
```

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 non-essential 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 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 single 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

1.11 EX16-ED-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221213
RULE ID: SV-221213r960933
```

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

1.12 EX16-ED-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221214
RULE ID: SV-221214r960936
```

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

1.13 EX16-ED-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange audit data must be on separate partitions.

```
GROUP ID: V-221215
RULE ID: SV-221215r960948
```

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)

1.14 EX16-ED-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange local machine policy must require signed scripts.

```
GROUP ID: V-221216
RULE ID: SV-221216r960954
```

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-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)

1.15 EX16-ED-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221218
RULE ID: SV-221218r1043178
```

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 Name, Identity, DomainSecureEnabled, DNSRoutingEnabled, RequireTLS, TlsAuthLevel
For each send connector:
If the send connector does not use a smarthost and the value of "DomainSecureEnabled" is not set to "True", this is a finding.
If the send connector does use a smarthost, "DomainSecureEnabled" will be set to "False".
If the send connector does use a smarthost "DNSRoutingEnabled", "RequireTLS", and "TlsAuthLevel" must be set.
If the send connector using a smart host has a value for “DNSRoutingEnabled” that is not set to “False”, this is a finding.
If the send connector using a smarthost has a value for “RequireTLS” that is not set to “True”, this is a finding.
If the send connector using a smarthost has a value for “TlsAuthLevel” that is not set to “DomainValidation”, this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:
Set-SendConnector <'IdentityName'> -DomainSecureEnabled $true
Note: The <IdentityName> value must be in single quotes.
Repeat the procedures for each send connector.
The following commands can be executed if smarthosts are used:
Set-SendConnector <'IdentityName'> -RequireTLS $true -DNSRoutingEnabled $False -TlsAuthLevel $DomainValidation

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

1.16 EX16-ED-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Internet-facing Send connectors must specify a Smart Host.

```
GROUP ID: V-221217
RULE ID: SV-221217r961101
```

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:

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 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 single quotes.
Repeat the procedures 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

1.17 EX16-ED-000180 (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-221219
RULE ID: SV-221219r1043178
```

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:

Open the Exchange Management Shell and enter the following command:
Get-ReceiveConnector | Select 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 single 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

1.18 EX16-ED-000190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Outbound Connection Timeout must be 10 minutes or less.

```
GROUP ID: V-221220
RULE ID: SV-221220r961155
```

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 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 single 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)

1.19 EX16-ED-000200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Outbound Connection Limit per Domain Count must be controlled.

```
GROUP ID: V-221221
RULE ID: SV-221221r961155
```

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 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 single 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)

1.20 EX16-ED-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange Send connector connections count must be limited.

```
GROUP ID: V-221222
RULE ID: SV-221222r961155
```

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 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 single 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)

1.21 EX16-ED-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange message size restrictions must be controlled on Send connectors.

```
GROUP ID: V-221223
RULE ID: SV-221223r961155
```

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 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 single 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 EX16-ED-000250 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange Send connectors delivery retries must be controlled.

```
GROUP ID: V-221224
RULE ID: SV-221224r961155
```

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 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 single 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 EX16-ED-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange Send connectors must be clearly named.

```
GROUP ID: V-221225
RULE ID: SV-221225r961155
```

Rationale:

For Send 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-SendConnector | Select Name, Identity
Review the naming for connectors.
For each send connector, 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-SendConnector -Name <'NewName'> -Identity <'IdentityName'>
Note: Both the <NewName> and <IdentityName> values must be in single quotes.
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)

1.24 EX16-ED-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Receive connector Maximum Hop Count must be 60.

```
GROUP ID: V-221226
RULE ID: SV-221226r961155
```

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 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 single 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 EX16-ED-000280 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange Receive connectors must be clearly named.

```
GROUP ID: V-221227
RULE ID: SV-221227r961155
```

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 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 single 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)

1.26 EX16-ED-000290 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

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

```
GROUP ID: V-221228
RULE ID: SV-221228r961155
```

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 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 single 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)

1.27 EX16-ED-000300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221229
RULE ID: SV-221229r961155
```

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 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 single 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)

1.28 EX16-ED-000310 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Exchange Internet Receive connector connections count must be set to default.

```
GROUP ID: V-221230
RULE ID: SV-221230r961155
```

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 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 single 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)

1.29 EX16-ED-000320 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Exchange Message size restrictions must be controlled on Receive connectors.

```
GROUP ID: V-221231
RULE ID: SV-221231r961155
```

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 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 single 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)

1.30 EX16-ED-000330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange messages with a blank sender field must be rejected.

```
GROUP ID: V-221232
RULE ID: SV-221232r961161
```

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 N/A for SIPR enclaves.
This requirement is N/A 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 Name, Action
If the value of "Action" is not set to "Reject", this is a finding.

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)

1.31 EX16-ED-000340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange messages with a blank sender field must be filtered.

```
GROUP ID: V-221233
RULE ID: SV-221233r961161
```

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 N/A for SIPR enclaves.
This requirement is N/A 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 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)

1.32 EX16-ED-000350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange filtered messages must be archived.

```
GROUP ID: V-221234
RULE ID: SV-221234r961161
```

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 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 single 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)

1.33 EX16-ED-000360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Sender filter must block unaccepted domains.

```
GROUP ID: V-221235
RULE ID: SV-221235r961161
```

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 blacklist 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 Deny 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 Name, BlockedDomains, BlockedDomainsAndSubdomains
If the value for "BlockedDomains" or "BlockedDomainsAndSubdomains" does not reflect the list of unaccepted 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>
Repeat the procedure for each domain that is to be blocked.
or
For BlockedDomainsAndSubdomains:
Set-SenderFilterConfig -BlockedDomainsAndSubdomains
<BlockedDomainAndSubdomain>
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)

1.34 EX16-ED-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange nonexistent recipients must not be blocked.

```
GROUP ID: V-221236
RULE ID: SV-221236r961161
```

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 non-existent 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 vs. nonexistent recipients.

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-RecipientFilterConfig | Select 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)

1.35 EX16-ED-000380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Sender Reputation filter must be enabled.

```
GROUP ID: V-221237
RULE ID: SV-221237r961161
```

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 antispam 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.
Open the Exchange Management Shell and enter the following command:
Get-SenderReputationConfig | Select 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)

1.36 EX16-ED-000390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221238
RULE ID: SV-221238r961161
```

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 antispam 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 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)

1.37 EX16-ED-000400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Attachment filtering must remove undesirable attachments by file type.

```
GROUP ID: V-221239
RULE ID: SV-221239r961161
```

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)

1.38 EX16-ED-000410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Spam Evaluation filter must be enabled.

```
GROUP ID: V-221240
RULE ID: SV-221240r961161
```

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.
Open the Exchange Management Shell and enter the following command:
Get-ContentFilterConfig | Select 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)

1.39 EX16-ED-000420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Block List service provider must be identified.

```
GROUP ID: V-221241
RULE ID: SV-221241r961161
```

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 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)

1.40 EX16-ED-000430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange messages with a malformed From address must be rejected.

```
GROUP ID: V-221242
RULE ID: SV-221242r1040907
```

Rationale:

Sender Identification (SID) is an email antispam 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 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)

1.41 EX16-ED-000470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange Recipient filter must be enabled.

```
GROUP ID: V-221243
RULE ID: SV-221243r961161
```

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 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-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)

1.42 EX16-ED-000480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange tarpitting interval must be set.

```
GROUP ID: V-221244
RULE ID: SV-221244r961161
```

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.

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 single 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)

1.43 EX16-ED-000490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internal Receive connectors must not allow anonymous connections.

```
GROUP ID: V-221245
RULE ID: SV-221245r961161
```

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 Name, Identity, PermissionGroups
For each Receive connector, if the value of "PermissionGroups" is "AnonymousUsers" for any non-Internet 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 single 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)

1.44 EX16-ED-000500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221246
RULE ID: SV-221246r961161
```

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 | fl
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)

1.45 EX16-ED-000510 (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-221247
RULE ID: SV-221247r961161
```

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

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)

1.46 EX16-ED-000520 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221248
RULE ID: SV-221248r961161
```

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 N/A for SIPR enclaves.
This requirement is N/A 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 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-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)

1.47 EX16-ED-000530 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have antispam filtering installed.

```
GROUP ID: V-221249
RULE ID: SV-221249r961161
```

Rationale:

Originators of spam messages are constantly changing their techniques in order 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 2016 provides both antispam and antimalware protection out of the box. The Exchange 2016 antispam and antimalware product capabilities are limited but still provide some protection.

Audit:

Review the Email Domain Security Plan (EDSP) for an installed antispam product.
Note: If using another DoD-approved antispam 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 AntiSpam module.
Open the Exchange Management Shell and enter the following command:
& $env:ExchangeInstallPath\Scripts\Install-AntiSpamAgents.ps1

Additional Information:

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

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

1.48 EX16-ED-000540 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have antispam filtering enabled.

```
GROUP ID: V-221250
RULE ID: SV-221250r961161
```

Rationale:

Originators of spam messages are constantly changing their techniques in order 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 2016 provides both antispam and antimalware protection out of the box. The Exchange 2016 antispam and antimalware product capabilities are limited but still provide some protection.

Audit:

Review the Email Domain Security Plan (EDSP) for an installed antispam product.
Note: If using another DoD-approved antispam 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)

1.49 EX16-ED-000550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have antispam filtering configured.

```
GROUP ID: V-221251
RULE ID: SV-221251r961161
```

Rationale:

Originators of spam messages are constantly changing their techniques in order 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 2016 provides both antispam and antimalware protection out of the box. The Exchange 2016 antispam and antimalware product capabilities are limited but still provide some protection.

Audit:

Site should utilize 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)

1.50 EX16-ED-000560 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange Sender Identification Framework must be enabled.

```
GROUP ID: V-221252
RULE ID: SV-221252r961161
```

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 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-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)

1.51 EX16-ED-000570 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-221253
RULE ID: SV-221253r961161
```

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 a DoD-approved protection mechanism such as Cloud Based Internet Isolation (CBII), Bromium, Email Gateway spamming device, such as Enterprise Email Security Gateway (EEMSG), or other approved email sanitization solution that protects against untrusted URLs embedded in email, 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' | FL
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)

1.52 EX16-ED-000580 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange application directory must be protected from unauthorized access.

```
GROUP ID: V-221254
RULE ID: SV-221254r961455
```

Rationale:

Default product installations may provide more generous access permissions than are necessary to run the application. By examining and tailoring access permissions to more closely provide the least amount of privilege possible, 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-001812 The information system prohibits user installation of software without explicit privileged status.

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

1.53 EX16-ED-000590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Exchange software baseline copy must exist.

```
GROUP ID: V-221255
RULE ID: SV-221255r961461
```

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)

1.54 EX16-ED-000610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221256
RULE ID: SV-221256r961470
```

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.

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)

1.55 EX16-ED-000620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221257
RULE ID: SV-221257r961608
```

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

1.56 EX16-ED-000630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221258
RULE ID: SV-221258r961620
```

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, Version: 6.0.3790.211 ready at Wed, 2 Feb 2005 23:40:00 -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 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 single 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

1.57 EX16-ED-000660 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Exchange must provide redundancy.

```
GROUP ID: V-221259
RULE ID: SV-221259r961620
```

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).
Determine if the Exchange servers are using redundancy by entering the following command:
Get-TransportService | select FL
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 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

1.58 EX16-ED-000670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange internal Send connectors must use an authentication level.

```
GROUP ID: V-221260
RULE ID: SV-221260r961620
```

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 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

1.59 EX16-ED-000680 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Exchange internal Receive connectors must require encryption.

```
GROUP ID: V-221261
RULE ID: SV-221261r961632
```

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 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 single 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

1.60 EX16-ED-000690 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Exchange internal Send connectors must require encryption.

```
GROUP ID: V-221262
RULE ID: SV-221262r961632
```

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 Name, Identity, TlsDomain
If the value of "TlsDomain" is not set to the value of the internal <'SMTP Domain'>, this is a finding.
Get-SendConnector | Select Name, Identity, DomainSecureEnabled
If the value of "DomainSecureEnabled" is not set to "True" and the SendConnector is not using a smarthost, this is a finding.
If the value of "DomainSecureEnabled" is set to "False" and the send connector is using a smarthost, the value of “RequireTLS” must be set to “True”, and the value for “TlsAuthLevel” must be set to “DomainValidation”.
If the send connector using a smarthost has a value for “RequireTLS” that is not set to “True”, this is a finding.
If the send connector using a smarthost has a value for “TlsAuthLevel” that is not set to “DomainValidation”, this is a Finding.

Remediation:

Open the Exchange Management Shell and enter the following command:
Set-SendConnector -Identity <'IdentityName'> -TlsDomain <'SMTP Domain'>
Set-SendConnector -Identity <'ReceiveConnector'> -DomainSecureEnabled 'True'
Note: The SMTP Domain is the internal SMTP domain within the organization.
The following commands can be executed if smarthosts are used:
Set-SendConnector <'IdentityName'> -RequireTLS $true -TlsAuthLevel $DomainValidation

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

1.61 EX16-ED-000700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Exchange must have the most current, approved service pack installed.

```
GROUP ID: V-221263
RULE ID: SV-221263r961683
```

Rationale:

The organization (including any contractor to the organization) must promptly install security-relevant software updates (e.g., patches, service packs, 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 | fl name, AdminDisplayVersion
If the value of "AdminDisplayVersion" does not return the most current, approved service pack, this is a finding.

Remediation:

Install the most current, approved service pack.

Additional Information:

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

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

1.62 EX16-ED-000720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must configure malicious code protection mechanisms to perform periodic scans of the information system every seven days.

```
GROUP ID: V-221264
RULE ID: SV-221264r961191
```

Rationale:

Malicious code protection mechanisms include, but are not limited, to anti-virus and malware detection software. In order to minimize potential negative impact to the organization that can be caused by malicious code, it is imperative that malicious code is identified and eradicated.

Malicious code includes viruses, worms, trojan horses, and spyware. It is not enough to simply have the software installed; this software must periodically scan the system to search for malware on an organization-defined frequency.

This requirement applies to applications providing malicious code protection.

Audit:

Open the Exchange Management Shell and enter the following command:
Get-TransportAgent "Malware Agent"
If the value of "Enabled" is set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:
& env:ExchangeInstallPath\Scripts\Disable-Antimalwarescanning.ps1

Additional Information:

CCI-001241 Configure malicious code protection mechanisms to perform periodic scans of the system on an organization-defined frequency.

- NIST SP 800-53::SI-3 c
- NIST SP 800-53A::SI-3.1 (vi)
- NIST SP 800-53 Revision 4::SI-3 c 1
- NIST SP 800-53 Revision 5::SI-3 c 1

1.63 EX16-ED-000730 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must configure malicious code protection mechanisms to perform periodic scans of the information system every seven days.

```
GROUP ID: V-221265
RULE ID: SV-221265r961191
```

Rationale:

Malicious code protection mechanisms include, but are not limited, to anti-virus and malware detection software. In order to minimize potential negative impact to the organization that can be caused by malicious code, it is imperative that malicious code is identified and eradicated.

Malicious code includes viruses, worms, trojan horses, and spyware. It is not enough to simply have the software installed; this software must periodically scan the system to search for malware on an organization-defined frequency.

This requirement applies to applications providing malicious code protection.

Audit:

Site must utilize an approved DoD third-party malicious code scanner.
Consult with System Administrator to demonstrate the application being used to provide malicious code protection in the Exchange implementation.
If System Administrator is unable to demonstrate a third-party malicious code protection application, this is a finding.
If System Administrator is unaware of a third-party malicious code protection application, this is a finding.

Remediation:

Following vendor best practice guidance, install and configure a third-party malicious code protection application.

Additional Information:

CCI-001241 Configure malicious code protection mechanisms to perform periodic scans of the system on an organization-defined frequency.

- NIST SP 800-53::SI-3 c
- NIST SP 800-53A::SI-3.1 (vi)
- NIST SP 800-53 Revision 4::SI-3 c 1
- NIST SP 800-53 Revision 5::SI-3 c 1

1.64 EX16-ED-000750 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must be configured to block and quarantine malicious code upon detection, then send an immediate alert to appropriate individuals.

```
GROUP ID: V-221266
RULE ID: SV-221266r961197
```

Rationale:

Malicious code protection mechanisms include, but are not limited, to anti-virus and malware detection software. In order to minimize potential negative impact to the organization that can be caused by malicious code, it is imperative that malicious code is identified and eradicated.

Applications providing this capability must be able to perform actions in response to detected malware. Responses include blocking, quarantining, deleting, and alerting. Other technology- or organization-specific responses may also be employed to satisfy this requirement.

Malicious code includes viruses, worms, trojan horses, and spyware.

This requirement applies to applications providing malicious code protection.

Audit:

Open the Exchange Management Shell and enter the following command:
Get-TransportAgent "Malware Agent"
If the value of "Enabled" is set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:
& env:ExchangeInstallPath\Scripts\Disable-Antimalwarescanning.ps1

Additional Information:

CCI-001243 Configure malicious code protection mechanisms to block malicious code; quarantine malicious code; and/or take organization-defined action(s) in response to malicious code detection.

- NIST SP 800-53::SI-3 c
- NIST SP 800-53A::SI-3.1 (vi)
- NIST SP 800-53 Revision 4::SI-3 c 2
- NIST SP 800-53 Revision 5::SI-3 c 2

1.65 EX16-ED-000760 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must be configured to block and quarantine malicious code upon detection, then send an immediate alert to appropriate individuals.

```
GROUP ID: V-221267
RULE ID: SV-221267r961197
```

Rationale:

Malicious code protection mechanisms include, but are not limited, to anti-virus and malware detection software. In order to minimize potential negative impact to the organization that can be caused by malicious code, it is imperative that malicious code is identified and eradicated.

Applications providing this capability must be able to perform actions in response to detected malware. Responses include blocking, quarantining, deleting, and alerting. Other technology- or organization-specific responses may also be employed to satisfy this requirement.

Malicious code includes viruses, worms, trojan horses, and spyware.

This requirement applies to applications providing malicious code protection.

Audit:

Site must utilize an approved DoD third-party malicious code scanner.
Consult with System Administrator to demonstrate the application being used to provide malicious code protection in the Exchange implementation.
If System Administrator is unable to demonstrate a third-party malicious code protection application, this is a finding.
If System Administrator is unaware of a third-party malicious code protection application, this is a finding.

Remediation:

Following vendor best practice guidance, install and configure a third-party malicious code protection application.

Additional Information:

CCI-001243 Configure malicious code protection mechanisms to block malicious code; quarantine malicious code; and/or take organization-defined action(s) in response to malicious code detection.

- NIST SP 800-53::SI-3 c
- NIST SP 800-53A::SI-3.1 (vi)
- NIST SP 800-53 Revision 4::SI-3 c 2
- NIST SP 800-53 Revision 5::SI-3 c 2

1.66 EX16-ED-002400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.

```
GROUP ID: V-221268
RULE ID: SV-221268r961188
```

Rationale:

Malicious code includes viruses, worms, trojan horses, and spyware. The code provides the ability for a malicious user to read from and write to files and folders on a computer's hard drive. Malicious code may also be able to run and attach programs, which may allow the unauthorized distribution of malicious mobile code. Once this code is installed on endpoints within the network, unauthorized users may be able to breach firewalls and gain access to sensitive data.

This requirement applies to applications providing malicious code protection. Malicious code protection mechanisms include, but are not limited, to, anti-virus and malware detection software. Malicious code protection mechanisms (including signature definitions and rule sets) must be updated when new releases are available.

Audit:

Open the Exchange Management Shell and enter the following command:
Get-TransportAgent "Malware Agent"
If the value of "Enabled" is set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:
& env:ExchangeInstallPath\Scripts\Disable-Antimalwarescanning.ps1

Additional Information:

CCI-001240 The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.

- NIST SP 800-53::SI-3 b
- NIST SP 800-53A::SI-3.1 (iii)
- NIST SP 800-53 Revision 4::SI-3 b

1.67 EX16-ED-002410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.

```
GROUP ID: V-221269
RULE ID: SV-221269r961188
```

Rationale:

Malicious code includes viruses, worms, trojan horses, and spyware. The code provides the ability for a malicious user to read from and write to files and folders on a computer's hard drive. Malicious code may also be able to run and attach programs, which may allow the unauthorized distribution of malicious mobile code. Once this code is installed on endpoints within the network, unauthorized users may be able to breach firewalls and gain access to sensitive data.

This requirement applies to applications providing malicious code protection. Malicious code protection mechanisms include, but are not limited, to, anti-virus and malware detection software. Malicious code protection mechanisms (including signature definitions and rule sets) must be updated when new releases are available.

Audit:

Site must utilize an approved DoD third-party malicious code scanner.
Consult with System Administrator to demonstrate the application being used to provide malicious code protection in the Exchange implementation.
If System Administrator is unable to demonstrate a third-party malicious code protection application, this is a finding.
If System Administrator is unaware of a third-party malicious code protection application, this is a finding.

Remediation:

Following vendor best practice guidance, install and configure a third-party malicious code protection application.

Additional Information:

CCI-001240 The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.

- NIST SP 800-53::SI-3 b
- NIST SP 800-53A::SI-3.1 (iii)
- NIST SP 800-53 Revision 4::SI-3 b

1.68 EX16-ED-003010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The applications built-in Malware Agent must be disabled.

```
GROUP ID: V-221270
RULE ID: SV-221270r961194
```

Rationale:

Malicious code protection mechanisms include, but are not limited, to, anti-virus and malware detection software. In order to minimize potential negative impact to the organization that can be caused by malicious code, it is imperative that malicious code is identified and eradicated.

Malicious code includes viruses, worms, trojan horses, and spyware. It is not enough to simply have the software installed; this software must periodically scan the system to search for malware on an organization-defined frequency.

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

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

Audit:

Open the Exchange Management Shell and enter the following command:
Get-TransportAgent "Malware Agent"
If the value of "Enabled" is set to "True", this is a finding.

Remediation:

Open the Exchange Management Shell and enter the following command:
& env:ExchangeInstallPath\Scripts\Disable-Antimalwarescanning.ps1

Additional Information:

CCI-001242 The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy.

- NIST SP 800-53::SI-3 c
- NIST SP 800-53A::SI-3.1 (vi)
- NIST SP 800-53 Revision 4::SI-3 c 1

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	EX16-ED-000010 (Manual)	☐	☐
1.2	EX16-ED-000020 (Manual)	☐	☐
1.3	EX16-ED-000030 (Manual)	☐	☐
1.4	EX16-ED-000050 (Manual)	☐	☐
1.5	EX16-ED-000060 (Manual)	☐	☐
1.6	EX16-ED-000070 (Manual)	☐	☐
1.7	EX16-ED-000080 (Manual)	☐	☐
1.8	EX16-ED-000090 (Manual)	☐	☐
1.9	EX16-ED-000100 (Manual)	☐	☐
1.10	EX16-ED-000110 (Manual)	☐	☐
1.11	EX16-ED-000120 (Manual)	☐	☐
1.12	EX16-ED-000130 (Manual)	☐	☐
1.13	EX16-ED-000140 (Manual)	☐	☐
1.14	EX16-ED-000150 (Manual)	☐	☐
1.15	EX16-ED-000170 (Manual)	☐	☐
1.16	EX16-ED-000160 (Manual)	☐	☐
1.17	EX16-ED-000180 (Manual)	☐	☐
1.18	EX16-ED-000190 (Manual)	☐	☐
1.19	EX16-ED-000200 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	EX16-ED-000230 (Manual)	☐	☐
1.21	EX16-ED-000240 (Manual)	☐	☐
1.22	EX16-ED-000250 (Manual)	☐	☐
1.23	EX16-ED-000260 (Manual)	☐	☐
1.24	EX16-ED-000270 (Manual)	☐	☐
1.25	EX16-ED-000280 (Manual)	☐	☐
1.26	EX16-ED-000290 (Manual)	☐	☐
1.27	EX16-ED-000300 (Manual)	☐	☐
1.28	EX16-ED-000310 (Manual)	☐	☐
1.29	EX16-ED-000320 (Manual)	☐	☐
1.30	EX16-ED-000330 (Manual)	☐	☐
1.31	EX16-ED-000340 (Manual)	☐	☐
1.32	EX16-ED-000350 (Manual)	☐	☐
1.33	EX16-ED-000360 (Manual)	☐	☐
1.34	EX16-ED-000370 (Manual)	☐	☐
1.35	EX16-ED-000380 (Manual)	☐	☐
1.36	EX16-ED-000390 (Manual)	☐	☐
1.37	EX16-ED-000400 (Manual)	☐	☐
1.38	EX16-ED-000410 (Manual)	☐	☐
1.39	EX16-ED-000420 (Manual)	☐	☐
1.40	EX16-ED-000430 (Manual)	☐	☐
1.41	EX16-ED-000470 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	EX16-ED-000480 (Manual)	☐	☐
1.43	EX16-ED-000490 (Manual)	☐	☐
1.44	EX16-ED-000500 (Manual)	☐	☐
1.45	EX16-ED-000510 (Manual)	☐	☐
1.46	EX16-ED-000520 (Manual)	☐	☐
1.47	EX16-ED-000530 (Manual)	☐	☐
1.48	EX16-ED-000540 (Manual)	☐	☐
1.49	EX16-ED-000550 (Manual)	☐	☐
1.50	EX16-ED-000560 (Manual)	☐	☐
1.51	EX16-ED-000570 (Manual)	☐	☐
1.52	EX16-ED-000580 (Manual)	☐	☐
1.53	EX16-ED-000590 (Manual)	☐	☐
1.54	EX16-ED-000610 (Manual)	☐	☐
1.55	EX16-ED-000620 (Manual)	☐	☐
1.56	EX16-ED-000630 (Manual)	☐	☐
1.57	EX16-ED-000660 (Manual)	☐	☐
1.58	EX16-ED-000670 (Manual)	☐	☐
1.59	EX16-ED-000680 (Manual)	☐	☐
1.60	EX16-ED-000690 (Manual)	☐	☐
1.61	EX16-ED-000700 (Manual)	☐	☐
1.62	EX16-ED-000720 (Manual)	☐	☐
1.63	EX16-ED-000730 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	EX16-ED-000750 (Manual)	☐	☐
1.65	EX16-ED-000760 (Manual)	☐	☐
1.66	EX16-ED-002400 (Manual)	☐	☐
1.67	EX16-ED-002410 (Manual)	☐	☐
1.68	EX16-ED-003010 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 5, 2025	1.0.0	Initial CIS Release