Resilient Infrastructure Security Warnings Reference

As part of Cisco's commitment to resilient infrastructure, a series of warning messages have been introduced into the Cisco IOS XE software to highlight potential security risks in a customer environment. These warning messages are broken up into one of two categories:

1. **Insecure Feature Warnings**: These warnings indicate that a configured feature or protocol does not meet modern security standards and is susceptible to attack. Insecure features should be considered deprecated and will be removed from the operating system in a future release. Customers should switch to more secure alternatives.

   When an insecure feature is enabled, the command line interface (CLI) on the device will display a warning message starting with **SECURITY WARNING**. Additionally, a message will be displayed in the syslog of the device (and sent to any configured remote syslog receivers). These logs will begin with **%SYS-4-INSECURE_CONFIG, %SYS-4-INSECURE_WARNING,** or **%SYS-4-INSECURE_DYNAMIC_WARNING**.

   Both the CLI and syslog warnings are typically followed by one or more of the following sections (not all messages include all the sections):
   a. **Module**: The IOS XE component that generated the log message, for example LOGGING, HTTP, or LINE
   b. **Command**: The specific command configured that triggered the warning message
   c. **Reason**: The reason why this feature or protocol is insecure
   d. **Description**: Additional details as to why the feature or protocol is insecure
   e. **Remediation**: Alternatives or action to take to migrate to a more secure alternative.

   For example:

   SECURITY WARNING - Module: SNMP, Command: snmp-server community * * , Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: SNMP community string configured - uses insecure SNMPv1/v2c protocol vulnerable to eavesdropping, Remediation:

Configure snmp v3 user

The above warning is displayed when an SNMPv2c community string is configured because SNMPv2 lacks encryption and uses weak authentication. The remediation suggests configuring SNMPv3 with authentication and encryption as an alternative.

2. **Security-Relevant Configuration Changes**: These warnings indicate that a critical configuration item has been modified which should be investigated by security teams if they are unexpected. For example, modification of AAA configuration could indicate an attacker attempting to circumvent authentication or authorization configurations or changes to logging configuration can indicate an attacker attempting to hide their activities by disabling or otherwise crippling visibility into their activities.

   These logging events may indicate expected configuration changes, in which case they can be ignored, but these events occurring in an environment where configuration changes are not being made intentionally should be investigated. These messages are all logged to syslog and have unique syslog prefixes such as %RADIUS-4-SERVER_ADDRESS_CHANGED or %TAC-4-AUTHENTICATION_PORT_CHANGED.

The remainder of this document includes references to possible log messages that may appear and additional details on the reasons for generating the warning as well as steps to take to mitigate the risk to the network.

Insecure Feature Warnings

As mentioned above, these warnings may appear on the CLI during configuration time, prefixed by SECURITY WARNING, or may appear in a syslog prefixed with **%SYS-4-INSECURE_CONFIG, %SYS-4-INSECURE _WARNING,** or **%SYS-4-INSECURE_DYNAMIC_WARNING**. The following section includes the text that follows the CLI or syslog prefix.

Warning Message: Module: LOGGING, Command: <shown below>, Reason: Weak tls version, Description: Logging TLS profile configured with TLS version 1.1 - deprecated and vulnerable to attacks, Remediation: Use stronger tls version to enhance security

Example Commands:

logging tls-profile <profile name>

tls-version TLSv1.1

Explanation: TLS 1.0 and TLS 1.1 (along with DTLS 1.0/1.1) were deprecated by RFC 8996 because these TLS versions no longer offer adequate security and are vulnerable to a variety of attacks. These versions of TLS should not be used.

Mitigation: TLS 1.2 or higher (with sufficiently strong cryptographic algorithms) should be used for any TLS communications. TLS 1.3 is recommended.

Warning Message: Module: LOGGING, Command: <shown below> , Reason: Weak cipher(s) are present in the command, Description: Logging TLS profile configured with weak cipher suite using CBC mode and SHA-1, Remediation: Use stronger cipher(s) to enhance security

Example Commands:

logging tls-profile <profile name>

ciphersuite <aes-128-cbc-sha | aes-256-cbc-sha>

Explanation: Cipher Block Chaining (CBC) mode ciphers are vulnerable to a variety of attacks and are considered insecure. Additionally, SHA1 is vulnerable to various attacks, posing a risk to data integrity. Neither CBC nor SHA1 should be used.

Mitigation: Use stronger, more modern ciphers that are not vulnerable to these kinds of attacks such as tls13-aes256-gcm-sha384.

Warning Message: %SYS-4-INSECURE_WARNING: service password-encryption. This configuration is not recommended and will be deprecated soon. Avoid using this command

Example Commands:

service password-encryption

Explanation: The service password-encryption command obfuscates credentials in a configuration file using a weak cipher that is easily reversed and does not provide adequate protection for credentials and other sensitive data in a configuration file. These obfuscated credentials are commonly referred to as “type 7” credentials.

Mitigation: Migrate to AES encryption of credentials (also known as “type 6” credentials) by using the command **service password-encryption aes**. Doing so requires the configuration of an encryption key using the **key config-key** command.

Warning Message: Module: HTTP, Command: ip http server , Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: HTTP server enabled - unencrypted protocol vulnerable to eavesdropping and man-in-the-middle attacks, Remediation: Use http secure server to ensure secure web access

Example Commands:
ip http server

Explanation: The HTTP protocol does not provide any protection for confidentiality or integrity and is therefore vulnerable to attacks.

Mitigation: Disable HTTP server and if the web server is needed, use HTTP over TLS (HTTPS) to protect traffic by configuring the **ip http secure-server** command.

Warning Message: Module: HTTP - Command: <see below> - Reason: Weak tls version - Remediation: Use stronger tls version to enhance security

Example Commands:
ip http tls-version <TLSv1.0/1.1>
ip http client tls-version <TLSv1.0/1.1>

Explanation: TLS 1.0 and TLS 1.1 (along with DTLS 1.0/1.1) were deprecated by RFC 8996 because these TLS versions no longer offer adequate security and are vulnerable to a variety of attacks. These versions of TLS should not be used.

Mitigation: TLS 1.2 or higher (with sufficiently strong cryptographic algorithms) should be used for any TLS communications. TLS 1.3 is recommended.

Warning Message: Module: HTTP - Command: <see below> - Reason: Weak cipher(s) are present in the command - Remediation: Use stronger cipher(s) to enhance security

Example Commands:
ip http secure-ciphersuite ecdhe-rsa-aes-128-cbc-sha
ip http secure-ciphersuite aes-128-cbc-sha
ip http secure-ciphersuite aes-256-cbc-sha
ip http client secure-ciphersuite aes-256-cbc-sha
ip http client secure-ciphersuite aes-128-cbc-sha

Explanation: Cipher Block Chaining (CBC) mode ciphers are vulnerable to a variety of attacks and are considered insecure. Additionally, SHA1 is vulnerable to a various attacks, posing a risk to data integrity. Neither CBC nor SHA1 should be used.

Mitigation: Use stronger, more modern ciphers that are not vulnerable to these kinds of attacks such as tls13-aes256-gcm-sha384.

Warning Message: Module: SANET, Command: <see below> , Reason: Weak cipher(s) are present in the command, Description: EAP profile configured with weak cipher suite using SHA-1 - vulnerable to collision attacks, Remediation: Use stronger cipher(s) to enhance security

Example Commands:
eap profile <profile name>
 ciphersuite aes128-sha
 ciphersuite aes256-sha
 ciphersuite dhe-rsa-aes128-sha
 ciphersuite dhe-rsa-aes256-sha
 ciphersuite ecdhe-ecdsa-aes-sha
 ciphersuite ecdhe-rsa-aes-sha

Explanation: Cipher Block Chaining (CBC) mode ciphers are vulnerable to a variety of attacks and are considered insecure. Additionally, SHA1 is vulnerable to a various attacks, posing a risk to data integrity. Neither CBC nor SHA1 should be used.

Mitigation: Use stronger, more modern ciphers that are not vulnerable to these kinds of attacks such as tls13-aes256-gcm-sha384.

Warning Message: Module: SANET, Command: <see below> , Reason: A weak authentication method is being configured as part of EAP profile, Description: EAP profile configured with weak authentication method MD5 or LEAP - vulnerable to dictionary attacks, Remediation: Please consider configuring a stronger method such as EAP-FAST, EAP-PEAP or EAP-TLS

Example Commands:
eap profile <profile name>
 method md5
 method leap

Explanation: MD5 is cryptographically weak and vulnerable to a variety of attacks including collision attacks and brute-force attacks. LEAP is also weak and vulnerable to dictionary attacks and other vulnerabilities.

Mitigation: Use a more secure protocol such as EAP-TLS or EAP-PEAP.

Warning Message: Module: SANET, Command: access-session tls-version 1.0 , Reason: Weak tls version, Description: Access session configured with TLS version 1.0 - deprecated and vulnerable to various attacks, Remediation: Use stronger tls version to enhance security

Example Commands:
access-session tls-version 1.0

Explanation: TLS 1.0 and TLS 1.1 (along with DTLS 1.0/1.1) were deprecated by RFC 8996 because these TLS versions no longer offer adequate security and are vulnerable to a variety of attacks. These versions of TLS should not be used.

Mitigation: TLS 1.2 or higher (with sufficiently strong cryptographic algorithms) should be used for any TLS communications. TLS 1.3 is recommended.

Warning Message: Module: FTP - Command: <see below> - Reason: No encryption is configured - Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols

Example Commands:
ip ftp passive
ip ftp password <password>
ip ftp source-interface <type> <string>
ip ftp username <string>

Explanation: The File Transfer Protocol (FTP) does not provide any protection for confidentiality or integrity and is therefore vulnerable to attacks.

Mitigation: Use secure protocols like SCP, SFTP, or HTTPS for file transfer operations. These protocols all provide strong authentication and encryption of data in transit.

Warning Message: Module: IP, Command: ip finger , Reason: IP Finger service can potentially expose system information to unauthorized users, Description: IP finger service enabled - provides system information that can be used for reconnaissance attacks, Remediation: Disable finger service and use secure SSH-based show commands for system information retrieval

Example Commands:
ip finger

Explanation: The finger protocol (RFC 742) is insecure and can expose system information without any authentication to a remote attacker which can be used for reconnaissance purposes. This protocol should not be used.

Mitigation: Retrieve system information through secure management protocols such as SSH or SNMPv3 (with authentication and encryption enabled).

Warning Message: Module: IP, Command: service finger , Reason: IP Finger service can potentially expose system information to unauthorized users, Description: Finger service

enabled - provides detailed user information that can be exploited for social engineering, Remediation: Disable finger service and use secure SSH-based show commands for system information retrieval

Example Commands:
service finger

Explanation: The finger protocol (RFC 742) is insecure and can expose system information without any authentication to a remote attacker which can be used for reconnaissance purposes. This protocol should not be used.

Mitigation: Retrieve system information through secure management protocols such as SSH or SNMPv3 (with authentication and encryption enabled).

Warning Message: Module: IP, Command: ip source-route , Reason: IP source routing allows attackers to bypass network security controls and routing policies, Description: IP source routing enabled - allows attackers to specify packet routing and bypass security controls, Remediation: This is a legacy feature, please consider disabling it

Example Commands:
ip source-route

Explanation: This command allows an IOS XE device to trust the contents of the Strict Source Route, Loose Source Route, Record Route, and Time Stamp IP header options, which are defined in RFC 791. This allows an attacker to affect how packets are routed through a network, potentially bypassing security controls like access lists or firewalls. This capability is not secure and should not be used because it allows untrusted end devices to determine packet routing.

Mitigation: Discontinue the use of this feature. Note that this does not affect other mechanisms available to perform routing decisions based on source IP address such as policy-based routing (PBR). PBR and similar mechanisms can be used safely, as these policies are determined by an administrator, not by an end client device.

Warning Message: Module: LINE, Command: <see below> , Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: Line transport configured with unencrypted protocols - allows plaintext transmission of sensitive data, Remediation: Migrate to secure SSH-based remote access

Example Commands:
line con 0
 transport output <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
 transport output all
 transport preferred <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>

telnet < break-on-ip | ip-on-break | refuse-negotiations | speed | sync-on-break | transparent >

line aux 0
transport output <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
transport input all
transport output all
transport input <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
transport preferred <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
telnet < break-on-ip | ip-on-break | refuse-negotiations | speed | sync-on-break | transparent >

line <line number or range>
transport output <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
transport input all
transport output all
transport input <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
transport preferred <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
telnet < break-on-ip | ip-on-break | refuse-negotiations | speed | sync-on-break | transparent >

line vty <line number or range>
transport output <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
transport input all
transport output all
transport input <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
transport preferred <pad | rlogin| telnet | acercon | lat | | mop | nasi | udptn | lapb-ta | v120>
telnet < break-on-ip | ip-on-break | refuse-negotiations | speed | sync-on-break | transparent >

Explanation: Legacy terminal access protocols other than SSHv2 like telnet do not provide adequate protection against data confidentiality and integrity and should not be used for remote access to a Cisco IOS XE device.

Mitigation: Use SSHv2 to access devices in conjunction with strong authentication, authorization, and accounting to validate and protect user access and provide strict role-based authorization.

Warning Message: Module: RCMD - Command: <see below> - Reason: No encryption is configured - Remediation: This is a legacy feature, please consider disabling it

Example Commands:
ip rcmd domain-lookup
ip rcmd rcp-enable
ip rcmd rsh-enable

ip rcmd remote-host
ip rcmd remote-username
ip rcmd rsh-disable-command
ip rcmd source-interface

Explanation: The Remote Copy Protocol (RCP) and Remote Shell Protocol (RSH) do not provide any protection for confidentiality or integrity and are therefore vulnerable to attacks. These protocols should not be used due to their lack of security.

Mitigation: Use secure protocols like SCP, SFTP, or HTTPS for file transfer operations or SSH for remote terminal access. These protocols all provide strong authentication and encryption of data in transit.

Warning Message: Module: TELNET - Command: service telnet-zeroidle - Reason: Telnet sessions are not configured with an idle timeout - Remediation: Migrate to secure SSH-based remote access

Example Commands:
service telnet-zeroidle

Explanation: Legacy terminal access protocols other than SSHv2 like telnet do not provide adequate protection against data confidentiality and integrity and should not be used for remote access to a Cisco IOS XE device. Additionally, configuring a terminal connection without an idle timeout presents a security risk if an idle session is left unattended.

Mitigation: Use SSHv2 to access devices in conjunction with strong authentication, authorization, and accounting to validate and protect user access and provide strict role-based authorization and ensure idle timeouts (recommendation is no more than 10 minutes) are configured for sessions.

Warning Message: Module: TELNET - Command: ip telnet comport disconnect delay 30 - Reason: IP traffic is not encrypted - Remediation: Migrate to secure SSH-based remote access

Example Commands:
ip telnet comport disconnect delay <>
ip telnet hidden <addresses | hostnames>
ip telnet quiet
ip telnet source-interface <>
ip telnet tos <0-FF>
ip telnet comport flow level
ip telnet comport receive window
ip telnet comport enable

Explanation: Legacy terminal access protocols other than SSHv2 like telnet do not provide adequate protection against data confidentiality and integrity and should not be used for remote access to a Cisco IOS XE device.

Mitigation: Use SSHv2 to access devices in conjunction with strong authentication, authorization, and accounting to validate and protect user access and provide strict role-based authorization and ensure idle timeouts (recommendation is no more than 10 minutes) are configured for sessions.

Warning Message: Module: TFTP - Command: <see below> - Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication - Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols

Example Commands:
ip tftp blocksize <>
ip tftp source-interface
ip tftp boot-interface

Explanation: The Trivial File Transfer Protocol (TFTP) does not provide any protection for confidentiality or integrity and is therefore vulnerable to attacks.

Mitigation: Use secure protocols like SCP, SFTP, or HTTPS for file transfer operations. These protocols all provide strong authentication and encryption of data in transit.

Warning Message: Reason: TCP small servers expose unnecessary network services and potential attack vectors - Remediation: Disable small servers and use modern network diagnostic tools like ping, traceroute, or SSH-based commands

Example Commands:
service tcp-small-servers

Explanation: TCP small servers (echo, chargen, discard, daytime) can be used by attackers to generate denial of service attacks and present an unnecessary attack surface. These services should not be used.

Mitigation: Discontinue the use of these features and use more modern diagnostic tools like ping, traceroute, and commands available in authenticated and encrypted management sessions like SSH.

Warning Message: Reason: UDP small servers expose unnecessary network services and potential attack vectors - Remediation: Disable small servers and use modern network diagnostic tools like ping, traceroute, or SSH-based commands

Example Commands:
service udp-small-servers

Explanation: UDP small servers (echo, chargen, discard, daytime) can be used by attackers to generate denial of service attacks and present an unnecessary attack surface. These services should not be used.

Mitigation: Discontinue the use of these features and use more modern diagnostic tools like ping, traceroute, and commands available in authenticated and encrypted management sessions like SSH.

Warning Message: Module: CDP - Command: router odr - Reason: On Demand Routing need to be disabled as in conjunction with cdp protocol static default routes will be added - Remediation: This is a legacy feature, please consider disabling it

Example Commands:
router odr

Explanation: On Demand Routing (ODR) is a legacy features that allows attackers to manipulate routing tables by sending unauthenticated, unencrypted CDP messages. This protocol is insecure and should not be used.

Mitigation: Use a routing protocol like OSPF, BGP, ISIS, or EIGRP with strong authentication configured to ensure routing updates are only performed by trusted systems.

Warning Message: Module: SNMP, Command: <see below> , Reason: Configuration employs an Insecure method for password storage, Description: SNMP user configured with weak privacy encryption DES/3DES - vulnerable to cryptographic attacks, Remediation: Use secure cipher such as aes

Example Commands:
snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <ipv6>
snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <1-99>
snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <std-acl>
snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <ipv6>
snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <1-99 >
snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <std-acl>

snmp-server user <> <> v3 encrypted auth (md5) access <ipv6 | (1-99) | std-acl>
snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <ipv6>
snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <(1-99)>
snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <std-acl>
snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <ipv6>
snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <(1-99) >
snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <std-acl>

Explanation: SNMPv3 traffic can be encrypted with a variety of ciphers. DES and 3DES ciphers are weak and vulnerable to a variety of attacks and should therefore not be used.

Mitigation: Use AES encryption for SNMPv3 traffic.

Warning Message: Module: SNMP, Command: <see below>, Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: SNMP community string configured - uses insecure SNMPv1/v2c protocol vulnerable to eavesdropping, Remediation: Configure snmp v3 user

Example Commands:
snmp-server community < > <ro|rw>
snmp-server community <0|7> < > <ro|rw> access <ipv6 | (1-99) | std-acl>
snmp mib community-map <0|7> <> context <> (engineid | security-name|target-list)

Explanation: SNMPv1 and SNMPv2c send sensitive data on the network without encryption including community strings used for authentication, allowing attackers to gain access to the sensitive data. If read-write capabilities are enabled, attackers can additionally modify network device configurations.

Mitigation: If SNMP is required, migrate to SNMPv3 with authentication and encryption enabled with strong cryptographic algorithms to manage network devices.

Warning Message: Module: SNMP, Command: <see below> , Reason: Insecure hash digest, Remediation: Use secure hash digest such as sha and sha-2

Example Commands:
snmp-server user <> <> v3 auth md5

Explanation: SNMPv3 authentication with MD5 relies on a weak cryptographic algorithm and is vulnerable to a variety of attacks such as brute force and collision attacks and should therefore not be used.

Mitigation: Use strong cryptographic ciphers like SHA2 for authenticating SNMPv3 traffic.

Warning Message: Module: SNMP, Command: <see below> , Reason: SNMP group with Auth/Noauth security level, Description: SNMP group configured with insufficient authentication level - missing privacy encryption, Remediation: Use SNMP group with Priv security level

Example Commands:
snmp-server group <> v3 <auth|noauth> access (ipv6| (1-99) | std-acl)

Explanation: SNMPv3 supports both authentication (auth) and encryption (priv). Both should be enabled to ensure secure communications. Authentication without encryption exposes sensitive data on the network.

Mitigation: If using SNMPv3, enable auth authentication and encryption with strong cryptographic algorithms to securely authenticate and encrypt the traffic.

Warning Message: Module: SNMP, Command: <see below>, Reason: SNMP host with Auth/Noauth security level, Description: SNMP host configured with insufficient authentication - missing privacy encryption, Remediation: Use SNMP host with Priv security level

Example Commands:
snmp-server host <> version {3} (auth|noauth) <username>
snmp-server host <> version (auth|noauth) <community> udp-port <0-65535>
snmp-server host <> vrf <1-65635> version {3} (auth|noauth) <username>
snmp-server host <> vrf <1-65635> version {3} (auth|noauth) <username> udp-port <0-65535>

Explanation: SNMPv3 supports both authentication (auth) and encryption (priv). Both should be enabled to ensure secure communications. Authentication without encryption exposes sensitive data on the network.

Mitigation: If using SNMPv3, enable auth authentication and encryption with strong cryptographic algorithms to securely authenticate and encrypt the traffic.

Warning Message: Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: SNMP host configured with

insecure version 1 or 2c - transmits data without encryption, Remediation: Configure snmp v3 user

Example Commands:
snmp-server host <> version {1|2c} * {0|7} <community>
snmp-server host <> version {1|2c} * {0|7} <community> udp-port <0-65535>
snmp-server host <> vrf <1-65535> version {1|2c}* {0|7} <community>
snmp-server host <> vrf <1-65535> version {1|2c} * {0|7} <community> udp-port <0-65535>

Explanation: SNMPv1 and SNMPv2c send sensitive data on the network without encryption including community strings used for authentication, allowing attackers to gain access to the sensitive data. If read-write capabilities are enabled, attackers can additionally modify network device configurations.

Mitigation: If SNMP is required, migrate to SNMPv3 with authentication and encryption enabled with strong cryptographic algorithms to manage network devices.

Warning Message: Module: SNMP, Command: <see below>, Reason: Insecure hash digest, Description: SNMP context user configured with MD5 authentication - vulnerable to collision attacks, Remediation: Use secure hash digest such as sha and sha-2

Example Commands:
snmp context abc user [^]+((credential|access|encrypted))? auth md5 [^]+(access)?
snmp context abc user [^]+(encrypted))? auth md5 [^]+(access)?
snmp context abc user [^]+((credential|access))? auth md5 [^]+(access)?
snmp context abc user [^]+(encrypted))? auth md5 [^]+(access)?
snmp context abc user [^]+(encrypted))? auth md5 [^]+ priv des (access)?
snmp context abc user [^]+((encrypted))? auth md5 [^]+ priv 3des (access)?

Explanation: SNMPv3 authentication with MD5 relies on a weak cryptographic algorithm and is vulnerable to a variety of attacks such as brute force and collision attacks and should therefore not be used.

Mitigation: Use strong cryptographic ciphers like SHA2 for authenticating SNMPv3 traffic.

Warning Message: Reason: Configuration employs an Insecure method for password storage, Description: SNMP context user configured with weak DES/3DES/DES56 privacy encryption - vulnerable to cryptographic attacks, Remediation: Use secure cipher such as aes

Example Commands:
snmp context abc user [^]+((credential|access|encrypted))? auth sha [^]+ priv des (access)?
snmp context abc user [^]+((credential|access|encrypted))? auth sha [^]+ priv 3des (

access)?
snmp context abc user [^]+((encrypted))? auth sha [^]+ priv des (access)?
snmp context abc user [^]+((encrypted))? auth sha [^]+ priv 3des (access)?
snmp context abc user [^]+ auth sha [^]+ priv des <> access <ipv6>
snmp context abc user [^]+ auth sha [^]+ priv 3des <> access <1-99>

Explanation: SNMPv3 traffic can be encrypted with a variety of ciphers. DES and 3DES ciphers are weak and vulnerable to a variety of attacks and should therefore not be used.

Mitigation: Use AES encryption for SNMPv3 traffic.

Warning Message: SECURITY WARNING - Module: SNMP, Command: snmp mib community-map abc context ctx, Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: SNMP MIB community map configured - exposes community strings in insecure SNMPv1/v2c, Remediation: Configure snmp v3 user

Example Commands:
snmp mib community-map abc context ctx

Explanation: SNMPv1 and SNMPv2c send sensitive data on the network without encryption including community strings used for authentication, allowing attackers to gain access to the sensitive data. If read-write capabilities are enabled, attackers can additionally modify network device configurations.

Mitigation: If SNMP is required, migrate to SNMPv3 with authentication and encryption enabled with strong cryptographic algorithms to manage network devices.

Warning Message: Module: SNMP, Command: <see below>, Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: SNMP group configured with insecure version 1 or 2c - lacks encryption and authentication, Remediation: Configure snmp v3 user

Example Commands:
snmp-server group <> v1
snmp-server group <> v2c

Explanation: SNMPv1 and SNMPv2c send sensitive data on the network without encryption including community strings used for authentication, allowing attackers to gain access to the sensitive data. If read-write capabilities are enabled, attackers can additionally modify network device configurations.

Mitigation: If SNMP is required, migrate to SNMPv3 with authentication and encryption enabled with strong cryptographic algorithms to manage network devices.

Warning Message: Module: BOOTP, Command: ip bootp server , Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: BOOTP server enabled - legacy protocol vulnerable to man-in-the-middle attacks and lacks security features, Remediation: Use DHCP to automatically configure network settings

Example Commands:
ip bootp server

Explanation: BootP is a legacy protocol vulnerable to various security weaknesses.

Mitigation: More modern protocols like DHCP can mitigate some of these weaknesses, especially when used in conjunction with protections like DHCP snooping. For bootstrapping devices, modern technologies like Secure Zero Trust Provisioning (Secure ZTP) can be used to securely onboard a device.

Warning Message: Module: SANET, Command: secure-webauth-disable , Reason: Secure web authentication is disabled, forcing insecure web-based authentication via HTTP, Description: Secure web authentication disabled - allows unencrypted HTTP authentication vulnerable to credential theft, Remediation: Remove secure-webauth-disable configuration to ensure secure web-based authentication via HTTPS

Example Commands:
secure-webauth-disable

Explanation: The HTTP protocol does not provide any protection for confidentiality or integrity and is therefore vulnerable to attacks. This command allows authentication traffic to be sent over the HTTP protocol which exposes those credentials on the network in an unencrypted format.

Mitigation: Remove the **secure-webauth-disable** command and ensure that HTTPS is enabled with a trusted certificate to protect authentication traffic on the network.

Warning Message: Module: NTP - Command: ntp authentication-key 1 md5 * - Reason: Weak cipher(s) are present in the command - Remediation: Transition to more secure algorithms like SHA and AES

Example Commands:
ntp authentication-key 1 md5 *

Explanation: MD5 is cryptographically weak and vulnerable to a variety of attacks including collision attacks and brute-force attacks. Attacks against NTP can lead to

outages of features reliant on accurate time such as those using X.509 certificates and can also lead to inaccurate logging timestamps.

Mitigation: Use a more secure cryptographic algorithm to protect NTP traffic such as hmac-sha2-256.

Warning Message: Module: SSH - Command: crypto key generate rsa … - Reason: SSH host key uses insufficient key length - Remediation: Use SSH RSA host key with a minimum length of 3072 bits for enhanced security

Example Commands:
crypto key generate rsa …

Explanation: The security of SSH sessions relies on host keys of sufficient length to defend against brute force attacks. RSA keys less than 2048 bits are considered weak today and in the near future, 3072 will be the minimum key size to protect against modern attacks.

Mitigation: To protect against future attacks, use RSA key sizes of at least 3072 bits or EC keys of at least 256 bits.

Warning Message: Module: SSH - Command: crypto key generate ec … - Reason: SSH host key uses insufficient key length - Remediation: Use SSH EC host key with a minimum length of 256 bits for enhanced security

Example Commands:
crypto key generate ec …

Explanation: The security of SSH sessions relies on host keys of sufficient length to defend against brute force attacks. EC keys less than 256 bits are considered weak.

Mitigation: To protect against future attacks, use RSA key sizes of at least 3072 bits or EC keys of at least 256 bits.

Warning Message: Module: SSH - Command: key-hash ssh-rsa * - Reason: Key is configured using insecure MD5 hash - Remediation: Configure the key using SHA-256 hash or via the key-string input method - Submode: configure - Parent CLI: ip ssh pubkey-chain; username <username>

Example Commands:
ip ssh pubkey-chain
 username <username>
 key-hash ssh-rsa A3453F0A611C53FEBBE3B3F58B7801EA

Explanation: Earlier versions of Cisco IOS XE stored key hashes in MD5 format. MD5 is vulnerable to various attacks including brute force and collision attacks. Newer versions of Cisco IOS XE store the hash using SHA2.

Mitigation: Re-enter the key using the key-string command which will re-generate the key-hash using SHA2.

Warning Message: Module: NTP - Command: <see below> - Reason: NTP configuration lacks authentication, allowing potential time manipulation attacks - Remediation: Configure a valid auth key and make it trusted using the command - ntp trusted-key

Example Commands:
ntp server <> key <num>
ntp peer <> key <num>
interface <>
 ntp broadcast <> key <num>
interface <>
 ntp multicast <> key <num>
no ntp authentication-key <num>

Explanation: Configuring NTP without a valid authentication key exposes NTP traffic to manipulation by attackers. Attacks against NTP can lead to outages of features reliant on accurate time such as those using X.509 certificates and can also lead to inaccurate logging timestamps.

Mitigation: Configure an NTP authentication key on the device and NTP server to provide strong authentication for NTP traffic.

Warning Message: Module: NTP - Command: <see below> - Reason: NTP configuration lacks authentication, allowing potential time manipulation attacks - Remediation: Please make the configured auth key trusted using the command - ntp trusted-key

Example Commands:
ntp server <> key <num>
ntp peer <> key <num>
interface <>
 ntp broadcast <> key <num>
interface <>
 ntp multicast <> key <num>
no ntp authentication-key <num>

Explanation: Configuring NTP without a valid authentication key exposes NTP traffic to manipulation by attackers. Attacks against NTP can lead to outages of features reliant on

accurate time such as those using X.509 certificates and can also lead to inaccurate logging timestamps.

Mitigation: Configure an NTP authentication key on the device and NTP server to provide strong authentication for NTP traffic.

Warning Message: Module: NTP - Command: <see below> - Reason: NTP configuration lacks authentication, allowing potential time manipulation attacks - Remediation: Configure ntp authenticate command to enable NTP authentication

Example Commands:
ntp server <> key <num>
ntp peer <> key <num>
interface <>
 ntp broadcast <> key <num>
interface <>
 ntp multicast <> key <num>
no ntp authenticate
no ntp authentication-key <num>

Explanation: Configuring NTP without a valid authentication key exposes NTP traffic to manipulation by attackers. Attacks against NTP can lead to outages of features reliant on accurate time such as those using X.509 certificates and can also lead to inaccurate logging timestamps.

Mitigation: Configure an NTP authentication key on the device and NTP server to provide strong authentication for NTP traffic.

Warning Message: Reason: TLS is not configured, exposing traffic to potential eavesdropping, Remediation: Configure secure options under server to enhance security

Example Commands:
radius server RADSER
 exit *(with no TLS commands associated with server)*

tacacs server TACSER
 exit *(with no TLS commands associated with server)*

ldap server LSERV
 exit *(without configuring secure LDAP)*

Explanation: The RADIUS, TACACS+, or LDAP server has been configured without sufficient authentication and encryption, potentially exposing sensitive credentials on the network.

Mitigation: For TACACS+, enable TACACS+ over TLS to protect TACACS+ traffic. For RADIUS, enable RADIUS over TLS (RadSec) or DTLS to protect RADIUS traffic. For LDAP traffic, enable **mode secure** to transport LDAP traffic over TLS.

Security-Relevant Configuration Changes

The following warnings are logged when specific configuration changes are made which may indicate a security issue like an attacker manipulating AAA or logging configuration. Customers should ensure these messages are monitored by network security teams to gain visibility into security-relevant configuration changes.

Warning Message: %AAA-4-USERNAME_CONFIGURATION: user with username: <username> configured

Example Commands:
username <user-name-string>
user-name <user-name-string>

Explanation: Indicates a local user was configured on a device. This can indicate an attacker is attempting to circumvent RADIUS or TACACS+ authentication by creating a local user and forcing authentication to use the local user database. Investigate the configuration change if it is unexpected.

Warning Message: %AAA-4-LOGIN_OR_ENABLE_MLIST_CHANGE: Login or enable mlist changed: Mlist string: authentication, service name: <service>

Example Commands:
aaa authentication login/enable <>

Explanation: Indicates a change to the AAA authentication list. This can indicate an attacker is attempting to circumvent RADIUS or TACACS+ authentication by changing the method used to authenticate users, for example bypassing TACACS+ authentication in favor of local authentication. Investigate the configuration change if it is unexpected.

Warning Message: %SEC_LOGIN-4-LOGIN_BLOCK_DISABLED: Login block feature is disabled at <timestamp>

Example Commands:
no login block-for <> attempts <> within <>

Explanation: The login block-for command prevents brute-force attacks by rate limiting the number of logins allowed over a period. This warning indicates that the login block feature has been disabled, possibly indicating an attempt to circumvent protections against brute force attacks. Investigate the configuration change if it is unexpected.

Warning Message: %RADIUS-4-SERVER_ADDRESS_CHANGED: Server: <server name>, Old address: <old IP address>, New address: <new IP address>

Example Commands:
radius server <server name>
 address ipv4 <new IP address>

Explanation: The server address for a RADIUS server has been changed. This can indicate an attacker is attempting to circumvent RADIUS authentication by pointing to an invalid or attacker-controlled RADIUS server to either force failover to local authentication or allow the attacker to permit authentications through a malicious RADIUS server. Investigate the configuration change if it is unexpected.

Warning Message: %RADIUS-4-AUTHENTICATION_PORT_CHANGED: Server: <server name or IP>, Old port: <port num>, New port: <port num>

Example Commands:
radius server RADSERV
 address ipv4 <server ip> auth-port <port num> acct-port <port num>

Explanation: The authentication port number for a RADIUS server has been changed. This can indicate an attacker is attempting to circumvent RADIUS authentication by pointing to an invalid port number to force failover to local authentication. Investigate the configuration change if it is unexpected.

Warning Message: %RADIUS-4-ACCOUNTING_PORT_CHANGED: Server: <server name or IP>, Old port: <port num>, New port: <port num>

Example Commands:
radius server RADSERV
 address ipv4 <server ip> auth-port <port num> acct-port <port num>

Explanation: The accounting port number for a RADIUS server has been changed. This can indicate an attacker is attempting to disable RADIUS accounting by pointing to an invalid port number, possibly to block the logging of any authentication or authorization activity. Investigate the configuration change if it is unexpected.

Warning Message: %TAC-4-SERVER_ADDRESS_CHANGED: Server: <server name>, Old address: <old IP address>, New address: <new IP address>

Example Commands:
tacacs server <server name>
 address ipv4 <new IP address>

Explanation: The server address for a TACACS+ server has been changed. This can indicate an attacker is attempting to circumvent TACACS+ authentication by pointing to an invalid or attacker-controlled TACACS+ server to either force failover to local authentication or allow the attacker to permit authentications through a malicious TACACS+ server. Investigate the configuration change if it is unexpected.

Warning Message: %TACACS-4-AUTHENTICATION_PORT_CHANGED: Server: <server name or IP>, Old port: <port num>, New port: <port num>

Example Commands:
tacacs server TACSERV
 port 1920

Explanation: The authentication port number for a TACACS+ server has been changed. This can indicate an attacker is attempting to circumvent TACACS+ authentication by pointing to an invalid port number to force failover to local authentication. Investigate the configuration change if it is unexpected.

Warning Message: % TACACS -4-ACCOUNTING_PORT_CHANGED: Server: <server name or IP>, Old port: <port num>, New port: <port num>

Example Commands:
tacacs server TACSERV
 port 1920

Explanation: The accounting port number for a TACACS+ server has been changed. This can indicate an attacker is attempting to disable TACACS+ accounting by pointing to an invalid port number, possibly to block the logging of any authentication or authorization activity. Investigate the configuration change if it is unexpected.

Warning Message: %LDAP-4-SERVER_ADDRESS_CHANGED: Server name: <server name>, Old address: <old IP address>, New address: <new IP address>

Example Commands:
ldap server <server name>
 ipv4 <new IP address>

Explanation: The server address for an LDAP server has been changed. This can indicate an attacker is attempting to circumvent LDAP authentication by pointing to an invalid or attacker-controlled LDAP server to either force failover to local authentication or allow the attacker to permit authentications through a malicious LDAP server. Investigate the configuration change if it is unexpected.

Warning Message: %LDAP-4-TRANSPORT_PORT_CHANGED: Server: <server name or IP>, Old port: <port num>, New port: <port num>

Example Commands:
ldap server <server name>
transport port <new port>

Explanation: The authentication port number for an LDAP server has been changed. This can indicate an attacker is attempting to circumvent LDAP authentication by pointing to an invalid port number to force failover to local authentication. Investigate the configuration change if it is unexpected.

Warning Message: %RADIUS-4-NON_TLS_SERVER_CONFIGURED: RADIUS server <server name> is configured without tls/dtls

Example Commands:
radius server <server name>
exit *(with no TLS commands associated with server)*

Explanation: A RADIUS server has been configured without TLS or DTLS. This could indicate an attacker has removed the TLS or DTLS configuration from a server previously configured to encrypt traffic, either breaking the connection or forcing the traffic to be sent without encryption (if the server is also accepting non-TLS connection). Investigate the configuration change if it is unexpected.

Warning Message: %TAC-4-NON_TLS_SERVER_CONFIGURED: TACACS+ server <server name>is configured without tls

Example Commands:
tacacs server <server name>
exit *(with no TLS commands associated with server)*

Explanation: A TACACS+ server has been configured without TLS. This could indicate an attacker has removed the TLS configuration from a server previously configured to encrypt traffic, either breaking the connection or forcing the traffic to be sent without encryption (if the server is also accepting non-TLS connection). Investigate the configuration change if it is unexpected.

Warning Message: %LDAP-4-NON_TLS_SERVER_CONFIGURED: LDAP server <server name> is configured without secure mode

Example Commands:
ldap server <server name>
exit *(with no secure mode configured)*

Explanation: An LDAP server has been configured without TLS. This could indicate an attacker has removed the TLS configuration from a server previously configured to encrypt traffic, either breaking the connection or forcing the traffic to be sent without encryption (if the server is also accepting non-TLS connection). Investigate the configuration change if it is unexpected.
