Resilient Infrastructure

Resilient Infrastructure

This project is designed to significantly strengthen the security posture of Cisco network devices by introducing a comprehensive, multi-layer security framework to reduce the attack surface and protect sensitive data through the implementation of new and improved security capabilities. Some of which may require our customers to act accordingly. We are committed to making this transition as seamless and non-disruptive as possible. Here's what else you need to know.

Strategy, Timeline, and Customer Readiness

- **Proactive Security Enhancements**: To increase the security posture of Cisco devices, we are making changes to default settings, deprecating and eventually removing insecure capabilities, and introducing new security features.
- **Your Action is Key**: We encourage all customers to adopt improved security practices now and discontinue the use of insecure features. This will strengthen your security posture and prepare you for these essential enhancements.
- **Comprehensive Guidance:** This playbook provides information on these changes, our strategy for phasing them out, and specific actions you should take.

For more information, see Resilient Infrastructure.

Deprecation of Insecure Features

Insecure features are being phased out in three stages to minimize disruption:

Stage 1: Warning

Warnings are displayed on the console when insecure features are configured. We strongly recommend discontinuing their use immediately.

Stage 2: Restriction

In subsequent releases, key insecure features will be disabled by default or require explicit administrator action to enable. Existing deployments continue to function, but new installations require intentional enablement.

Some features on specific platforms may not have a restriction phase, with only warnings continuing for several releases before removal.

Stage 3: Removal

Obsolete features are planned to be removed entirely from future software releases.

The timing of removal will vary based on user impact and adoption (e.g., widely adopted features like SNMPv2 will phase out slower than less-used ones).

For more information, see the respective software Release Notes.

NFVIS

NFVIS is already aligned with our security goals in 4.18.2, requiring no specific changes for this release. These are the changes in Release 26.1.1:

- Weak Cipher
- Type 6 Encryption

- Default Password
- AAA/Radius/TACACS
- SNMP
- Smart Licensing
- FTP
- HTTP
- Bulk Encryption- Password Encryption

Weak Cipher

Weak ciphers are encryption algorithms used to secure data transmissions that are considered insecure or vulnerable for various reasons.

What's Changing?

Insecure Ciphers such as DES, SHA, and MD5 are flagged as insecure in nfvisEvent and syslog.

What to do next?

Remediate by updating SNMP user configuration to use SHA-256 for authentication and AES for privacy instead of MD5 and DES.

Syslog entry when using insecure ciphers

```
nfvis# show log nfvis_syslog.log
2025-11-25T05:10:42.433240+00:00 nfvis %SYS-6-SNMP_INSECURE_PROTOCOL: SNMP user test is
configured with insecure auth protocol 'md5'. Use sha256.
2025-11-25T05:10:42.440765+00:00 nfvis %SYS-6-SNMP_INSECURE_PROTOCOL: SNMP user test is
configured with insecure priv protocol 'des'. Use aes.
```

Warning Message

```
nfvis# show system insecure_configuration
system insecure_configuration modules SNMP_HOST_VERSION
description  "Snmp configured version for the host."
remediation  "Use SNMPv3 for secure host configurations."
cli_template "snmp host {host} host-version {version}"
reason       "SNMPv3 provides enhanced security features for SNMP hosts."
system insecure_configuration modules SNMP_HOST_SECURITY_LEVEL
description  "Snmp security level for the host."
remediation  "Use 'authPriv' security level for SNMP groups."
cli_template "snmp host {host} host-security-level {host-security-level}"
reason       "The 'authPriv' security level ensures both authentication and privacy."
```

Type 6 Encryption

Type 6 Encryption in Cisco devices refers to a password encryption method that uses a reversible 128-bit Advanced Encryption Standard (AES) symmetric cipher. This encryption type allows passwords and keys to be stored securely in an encrypted format on the device while still enabling the device to decrypt them back to their original plain-text form when needed for operations.

What's Changing?

Sensitive credentials stored as plaintext (Type 0) are now insecure.

What to do next?

Use automated Type-6 encryption to upgrade your credential security. Type-6 encryption applies AES-based keys and a user-defined master key (which is not stored in the device configuration) to convert plaintext (Type-0) keys into securely encrypted keys. This action enhances Cisco infrastructure security and simplifies key management. Transition all existing plaintext credentials to Type-6 encrypted format to maintain compliance and protect sensitive data.

Default Password

The default password refers to the initial password set on a device or system before it is configured by the user. For Cisco products, default passwords vary depending on the device or system.

What's Changing?

Devices no longer use default credentials (such as cisco/cisco).
Additionally, credentials are now excluded from debug output logs to improve security.

What to do next?

When prompted, change the default password to a strong, unique password during initial setup.

AAA/RADIUS/TACACS

AAA is a security framework for managing user access and tracking, with RADIUS as an open standard protocol combining authentication and authorization using UDP and limited encryption. TACACS+ is a Cisco proprietary protocol using TCP that separates authentication, authorization, and accounting with full packet encryption and granular command control

What's Changing?

NFVIS now stores both shared-secret and encrypted-shared-secret values in encrypted form for TACACS+ and RADIUS. There are new constraints on secret length and allowed characters.

What to do next?

Configure TACACS+ and RADIUS shared secrets with a length between 1 and 127 characters using only allowed characters, and apply them via the **shared-secret** or **encrypted-shared-secret** commands followed by **commit**.

Running configuration for Radius

```
nfvis# show running-config radius-server
radius-server host 1.2.3.4
shared-secret $8$lZwgccBvs9x1oQpx6f1s8/JkZ4rLdQ95VMUjRrhD9Z8=
admin-priv    15
oper-priv     11
```

Radius-server and TACACS server secrets are in encrypted form when saved to the configuration database (CDB).

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for communication between SNMP managers and agents to monitor and manage network devices.

What's Changing?

SNMPv1, SNMPv2, SNMPv3 (noAuthNoPriv) are insecure SNMP configurations.

You are blocked from configuring the above in secure mode. Enable insecure mode using the **system mode insecure** command, which then triggers warnings.

What to do next?

Migrate to SNMPv3 using authPriv security level with strong authentication (e.g., SHA256) and privacy (e.g., AES). Enable insecure mode only as a temporary bridge for legacy configurations.

Sample Syslog

```
nfvis# show log nfvis_syslog.log
2025-11-10T08:20:09.936370+00:00 nfvis %SYS-6-SNMP_INSECURE_VERSION: SNMP user test uses insecure version v1.
2025-11-10T08:20:09.955272+00:00 nfvis %SYS-6-SNMP_INSECURE_PROTOCOL: SNMP user test is configured with insecure auth protocol 'md5'. Use sha256.
2025-11-10T08:20:09.978451+00:00 nfvis %SYS-6-SNMP_INSECURE_PROTOCOL: SNMP user test is configured with insecure priv protocol 'des'. Use aes.
```

Warning message when SNMPv1 is configured

```
nfvis# show system mode
system mode status secure
nfvis(config)# snmp user test user-version 1 user-group test_group auth-protocol md5 priv-protocol des passphrase qwertyuiop encryption-passphrase qwertyuiop
nfvis(config-user-test)# commit
Aborted: 'snmp user test user-version': SNMP Version 1 is insecure. Enable insecure mode to configure this.
```

Smart Licensing

Smart Licensing is a cloud-based software license management solution that simplifies the activation, management, and tracking of Cisco software licenses across an organization.

What's Changing?

HTTP protocol cannot be used for configuring connection to Cisco SSM or CSLU

```
license smart transport smart smart-url < >
license smart transport cslu cslu-url < >
```

What to do next?

Use HTTPS to establish a connection to Cisco SSM or CSLU

```
license smart transport smart smart-url https://<custom URL>
```

Console Message

```
nfvis(config)# license smart transport cslu cslu-url http://cslu.cisco.com
nfvis(config-smart)# commit
Aborted: http protocol for licensing transport url can only be configured in insecure mode.
nfvis(config-smart)#
```

Sample Syslog

```
nfvis# show log nfvis_syslog.log
2025-07-23T10:03:32.036119+00:00 nfvis %SYS-6-INSECURE_LICENCE_CONFIGURATION: http protocol
for licensing transport url can only be configured in insecure mode. HTTP protocol is used
for license configuration
```

FTP and TFTP

FTP and TFTP are both protocols used for transferring files over a network.

What's Changing?

NFVIS issues warning message when FTP or TFTP protocols are used for file transfer.

What to do next?

Use secure protocol such as HTTPS or SCP for file transfers.

```
scp root@172.25.213.123:/mnt/Volume2/nfs_share_esclite/<image> intdatastore:<image>
```

Console Message

```
nfvis(config)# vm_lifecycle images image jx src ftp://1.1.1.1:/home/a properties property a
nfvis(config-property-a)# commit
Aborted: Image [jx] uses legacy protocol [FTP] for source [ftp://1.1.1.1:/home/a]. Consider
using secure protocols like SCP/HTTPS.
```

Sample Syslog

```
show log nfvis_syslog.log:
2025-11-21T06:09:46.035182+00:00 nfvis %SYS-6-LEGACY_PROTOCOL_WARNING: Legacy protocol
warning successful: Warning: Image [jx] uses legacy protocol [FTP] for source
[ftp://10.197.82.5:/E1100D-FOC27080VDN-20240129-230104.tar.gz]. Consider using secure
protocols like SCP/HTTPS.
```

HTTP

HTTP is a standard protocol used for unencrypted traffic between web browsers and servers.

What's Changing?

NFVIS issues a warning message when you download the upgrade-image and VM image through HTTP.

What to do next?

Use HTTPS for file downloads.

Sample Syslog

```
nfvis# show log nfvis_syslog.log

2025-11-10T04:08:36.602807+00:00 nfvis %SYS-6-SYSTEM_MODE_UPDATED: System mode updated
System mode insecure mode is removed

2025-11-10T12:54:27.603595+00:00 nfvis %SYS-6-SYSTEM_MODE_UPDATED: System mode updated
System mode changed to insecure

2025-11-10T12:54:39.573343+00:00 nfvis %SYS-6-LEGACY_PROTOCOL_CONFIGURED: Insecure
configuration detected Legacy protocol http is used for file download, please use the local
datastore
```

Bulk Encryption- Password Encryption

Bulk password encryption refers to the process of encrypting multiple passwords simultaneously, typically during configuration or deployment tasks, to enhance security by preventing clear-text password exposure.

What's Changing?

For standalone NFVIS deployment, SNMP community string is hidden from the user in show running config. For NFVIS vBranch, the community string in SNMP won't be hidden as vManage does not hide or encrypt the community string configured by user.

Running configuration with encrypted password for TACACS

```
nfvis# show running-config tacacs-server

tacacs-server host 1.2.3.4
shared-secret $8$JkMZFgA3DkbjAHOrmdBr3U2cLg2qY1FuHAIJiIp7nSw=
admin-priv    15
oper-priv     11
```

Running configuration with hidden community strings in NFVIS standalone deployment

```
nfvis# show running-config snmp

snmp agent engineID 00:00:00:09:00:00:ec:f4:0c:0d:48:36

snmp community ****

community-access ****
```