Update CIMC Firmware on Cisco Secure Web Appliances

Contents

This firmware update package is to update the Cisco Integrated Management Controller (IMC) firmware, which has the fix for the vulnerabilities detailed in CVE-20240-20295 and CVE-2024-20356.

Note: The update for Cisco IMC firmware is available only for appliances that require the upgrade. If you are running a supported version of AsyncOS and you do not see the upgrade package with the description **Firmware update package Cisco IMC CVE-2024-20295 CVE-2024-20356** in the list of available upgrades, you can assume that your appliance does not require the upgrade and skip this upgrade process.

Appliances Covered by Cisco IMC Firmware Update

- S195, S395, S695/F
- S196, S396, S696/F

Supported Software Versions for Cisco IMC Firmware Update

If you are running an AsyncOS version that is not listed in this section, upgrade your AsyncOS to any of the below versions before installing the firmware patch:

- 15.0.0-355
- 15.1.0-287
- 15.2.0-116
- 15.2.0-164

Update for CIMC Firmware Installation Instructions

Follow the instructions below to obtain and install the update for CIMC firmware patch.

Note: In this process and document, "upgrade" and "update" are used interchangeably.

Pre-installation Requirements

Before you install the update for CIMC firmware, save the configuration file to a location on the appliance:

Step 1. In the graphical user interface, navigate to **System Administration > Configuration File**.

Step 2. In the **Current Configuration** tab, do the following:

a. Select **Download file to local computer to view or save**.

b. Under **Password Display Options**, select **Encrypt passwords in the Configuration Files** and then specify how to generate the file name. You can either select **Use system-generated file name** or **Use user-defined file name**. If you are selecting **Use user-defined file name**, enter the file name.

Step 3. Click **Submit**.

Installing the CIMC Firmware Update

Step 1. Access the CLI interface. For details on accessing the CLI, see Cisco Secure Web Appliance User Guide.

Note: For the update to run successfully, you must run the upgrade from the CLI.

Step 2. Select *DOWNLOADINSTALL* option. You must only select *DOWNLOADINSTALL* option for this update to work properly.

Step 3. From the CLI enter upgrade.

Step 4. Select the CIMC update package from the upgrade package list. Enter the number with the description - **Firmware update package Cisco IMC CVE-2024-20295 CVE-2024-20356**.

Step 5. You are prompted to save the current configuration to the configuration directory. The default value is Y (yes). Enter *N* if you do not want to save the current configuration.

Step 6. Choose the password option from the list and press enter.

Step 7. Enter *Y* when prompted to proceed with the update.

The following message will be displayed :

```
BMC firmware update:
====================
    Updating BMC from 4.0(1e) to 4.2(3j). This may take some time please wait...
    BMC Update complete
    Activating BMC. Please wait...
    CIMC login will be disconnected, Please connect after two mins
    Activation of BMC firmware successful
    Current running version of BMC: 4.2(3j)
Upgrade installation finished.
```

Note: CIMC firmware update does not require a reboot. The system will not reboot after the upgrade process.

Note: The firmware update package will be displayed in the list of available upgrades even after successful installation. This does not indicate that the firmware upgrade was unsuccessful.

Step 8. (Optional) Verify the CIMC firmware update using the version command. If the BMC version is updated to 4.02, it indicates that the update was successful.

Note: If the update fails even after multiple tries, contact Cisco TAC for assistance.

Example:

```
UDI: S195 VA0 WZP231206NK
Name: S195
Product: Cisco S195 Secure Web Appliance
Model: S195
Version: 15.0.0-355
Build Date: 2023-07-12
Install Date: 2023-07-12 15:28:41
Serial #: D4789B004502-WZP231206NK
BIOS: C220M5.4.0.1h.0.1108182337
RAID: 50.1.0-1456
RAID Status: Optimal
RAID Type: 1
BMC: 4.02
Cisco DVS Engine: 1.0 (Never Updated)
Cisco DVS Malware User Agent Rules: 0.554 (Never Updated)
Cisco DVS Object Type Rules: 0.554 (Never Updated)
Cisco Trusted Root Certificate Bundle: 2.4 (Tue Jun 04 19:22:28 2024)
Cisco Certificate Blocked List: 1.3 (Tue Jun 04 19:22:28 2024)
How-Tos: 1.0 (Never Updated)
Youtube Categorization engine: 1.0.0 (Never Updated)
```

Related Content

This document describes and provides links to the hardware and software user documentation available for Secure Web Appliances. To find a document online, use one of the links in this section.

Documentation	Location
User Guide for Cisco Web Security Appliances	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html
Secure Web Appliance Release Notes, ISE Compatibility Matrix, and Ciphers	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
Hardware Installation and Getting Started guides for Secure Web Appliances	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

Support

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.

Access the Cisco Support Community at the following URLs:

https://supportforums.cisco.com/community/5786/web-security

Legal Information