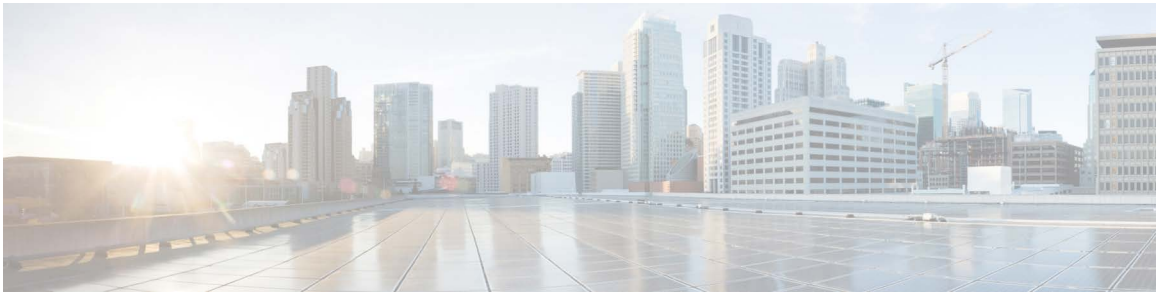

Firmware Update for x95 Series Cisco Secure Email Gateway and Cisco Secure Email and Web Manager

Published: June 21, 2024

Contents

Introduction

A vulnerability has been discovered in the CLI of the Cisco Integrated Management Controller (IMC). This vulnerability could potentially allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and gain root privileges. This firmware update package contains the fix for this vulnerability.

Note It may take up to two hours for the upgrade process to finish. Please do not turn off or shut down the machine.

Cisco Systems, Inc.
www.cisco.com

Appliances Covered by the Firmware Update

- C195, C395, C695, C695F
- M195, M395, M695, M695F

Firmware Update Package Version

Cisco IMC CVE-2024-20295 CVE-2024-20356

Supported AsyncOS Versions for the Firmware Update

If you are running an AsyncOS version that is not listed in this section, upgrade AsyncOS to a supported release before installing the firmware patch.

Secure Email Gateway	Secure Email and Web Manager
• 15.0.0-104 • 15.0.1-030 • 15.5.1-055	• 15.0.0-413 • 15.5.1-024

Fixed Issues

- CSCwi43005: Cisco IMC Web-Based Management Interface Command Injection Vulnerability.

Firmware Update Installation Instructions

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

Pre-installation Requirements

Before you install the update for firmware, save the configuration file to a location off of the gateway:

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

Step 2 Select **Download file to local computer to view or save**.

Step 3 Click **Submit**.

Installing the Firmware Update

Prerequisites:

- Reboot the Secure Email Gateway and/or Secure Email and Web Manager.
- Check the firmware version on your Secure Email Gateway and/or Secure Email and Web Manager. To check the versions on your gateway, type `version` in the command line interface (CLI). For details on accessing the CLI, see Accessing the CLI.
  Here is an example of the CLI version output (before upgrade):

```
mail.example.com> version

Current Version

===============

UDI: C695 VA0 12345ABCDEF

Name: C695

Product: Cisco C695 Email Security Appliance

Model: C695

Version: 15.0.1-030

Build Date: 2023-11-19

Install Date: 2024-02-08 12:43:47

Serial #: ABCDEF123456-12345ABCDEF

BIOS: C220M5.4.0.1h.0.1108182337

RAID: 50.1.0-1456

RAID Status: Optimal

RAID Type: 10

BMC: 4.00
```

- The latest versions are:
  - BIOS: *4.3.2a*
  - RAID: *51.19.0-4532*
  - BMC: 4.2(3j)

Note

- If you are using a supported AsyncOS version listed in Supported AsyncOS Versions for the Firmware Update, page 2, but your firmware versions are not up to date, you must download and install the firmware update patch.
- If you are not using any of the supported AsyncOS versions, you need to first upgrade your AsyncOS version to one of the supported versions and then apply the firmware update patch.
- Contact Cisco TAC for assistance with provisioning.

Note For the upgrade to run correctly, you *must* run it from the CLI.

Step 1 In the Command Line Interface, type `upgrade.`

Step 2 Type `downloadinstall.`

Step 3 A list of available upgrades will display.

Step 4 Select the *Firmware update package*.

Step 5 You will be prompted to reboot your machine. Click **Yes**.

Step 6 Wait approximately fifteen minutes.

Step 7 Your machine should automatically reboot after approximately fifteen minutes.

⚠

Caution If your machine does not automatically reboot in fifteen minutes, contact customer support. Do not attempt to reboot your machine again.

Here is an example of the CLI output:

```
mail.example.com > upgrade

Are you sure you want to proceed with upgrade? [N]> y

Choose the operation you want to perform:

- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs
reboot).

- DOWNLOAD - Downloads the upgrade image.

[]> downloadinstall

You must disconnect all machines in the cluster in order to upgrade
them. Do you wish to disconnect all machines in the cluster now? [Y]>
y

Upgrades available.

1. AsyncOS 15.5.1 build 024 upgrade For Email, 2024-04-30, is a
release available as General Deployment.

2. ...

3. ...

.

.

12. Firmware update package Cisco IMC CVE-2024-20295 CVE-2024-20356

[12]> 12

Would you like to save the current configuration to the configuration
directory before upgrading? [Y]> y

Would you like to email the current configuration before upgrading?
[N]> n

Choose the password option:

1. Mask passwords (Files with masked passwords cannot be loaded using
loadconfig command)

2. Encrypt passwords

[1]> 2
```

```
After you upgrade to AsyncOS 11.0 or later, the appliance generates
a unique certificate. The existing demo certificate is replaced with
the new certificate. However this does not apply for AsynOS 11.4.If
it fails to generate the unique certificate, the demo certificate
will be used.

Since version 12.0, the Next Generation portal of your appliance by
default uses AsyncOS API HTTP/HTTPS ports (6080/6443) and
trailblazer HTTPS port (4431). You can configure the HTTPS (4431)
port using the trailblazerconfig command in the CLI. Make sure that
the configured HTTPS port is opened on the firewall and ensure that
your DNS settings can resolve the hostname that you specified for
accessing the appliance.

Performing an upgrade may require a reboot of the system after the
upgrade is applied. You may log in again after the upgrade is done.

Do you wish to proceed with the upgrade? [Y]> y

During the upgrade, you may observe messages related to IPMI. You
can ignore these messages.

Upgrade payload extracted.

BIOS is upgrading from 4.0.1h to 4.3.2a

BMC is upgrading from 4.0(0) to 4.2(3j)

RAID is upgrading from 50.1.0-1456 to 51.19.0-4532

Configuring Firmware upgrade after reboot

0132+0 records in

0132+0 records out

364010752 bytes transferred in 0.826913 secs (802999605 bytes/sec)

reboot partition configured

Firmware upgrade after reboot scheduled

---

WARNING -

New BIOS, BMC and RAID firmwares will be upgraded. This appliance
will reboot, then install the new firmwares.

It is important that you do not power-cycle or interrupt the
appliance this time. If 2 hours has elapsed without the machine
coming back up, it has run into a problem and you will need to do a
manual reboot.

If a problem still persists or the upgrade is not successful please
contact tac@cisco.com

Upgrade installation finished.

Reboot takes about 20 minutes to complete. Do not interrupt power to
the appliance during this process.

Enter the number of seconds to wait before forcibly closing
connections. [30]> 0
```

Note After you run the firmware upgrade, the firmware upgrade package will display in the list of available upgrades even after a successful installation. The presence of this package does *not* indicate a failed upgrade.

Step 8 To verify that the upgrade has run successfully, you can run the upgrade script again after the machine has rebooted. If the upgrade was successful, the upgrade script will indicate that the appliance does not require upgrading.

- Here is an example of the CLI version output (after upgrade):

```
mail.example.com> version
Current Version
===============
UDI: C695 VA0 12345ABCDEF
Name: C695
Product: Cisco C695 Email Security Appliance
Model: C695
Version: 15.0.1-030
Build Date: 2023-11-19
Install Date: 2024-02-08 12:43:47
Serial #: ABCDEF123456-ABCDEF12345
BIOS: C2405.4.3.2a.0.0613231011
RAID: 51.19.0-4532
RAID Status: Optimal
RAID Type: 10
BMC: 4.02
```

Accessing the CLI

To run this upgrade, you must access the CLI. The instructions below provide information on accessing the CLI.

Access to the CLI varies depending on the management connection method chosen while setting up the appliance. Initially, only the admin user account has access to the CLI. You can add other users with differing levels of permission after you have accessed the command line interface for the first time via the admin account. The system setup wizard asks you to change the password for the admin account. The password for the admin account can also be reset directly at any time using the password command. To connect via Ethernet: Start an SSH or Telnet session with the factory default IP address 192.168.42.42. SSH is configured to use port 22. Telnet is configured to use port 23.

To connect via a Serial connection: Start a terminal session with the communication port on your personal computer that the serial cable is connected to. See the “Setup and Installation” chapter in the *User Guide for AsyncOS for Cisco Secure Email Gateway* for more information. Enter the user name and password below.

Factory Default User name and Password

- Username: `admin`
- Password: `ironport`

Support

Cisco Support Community

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 URL:

https://community.cisco.com/t5/email-security/bd-p/5756-discussions-email-security

Customer Support

Use the following methods to obtain support:

U.S.: Call 1 (408) 526-7209 or Toll-free 1 (800) 553-2447

International: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Support Site: https://www.cisco.com/c/en/us/support/index.html

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.