Cisco Secure Endpoint Private Cloud Firmware Upgrade for CVE-2024-20356

Contents

Introduction

Remediation of CVE-2024-20356 requires an update to the CIMC firmware for the Cisco Secure Endpoint Private Cloud appliance. This article describes the process of upgrading the firmware of a Private Cloud UCS appliance.

Prerequisites

- Secure Endpoint Private Cloud UCS Appliance with Private Cloud version 3.9.x or above.
- Access to the Private Cloud UCS Appliance CIMC web UI (including access to the web based KVM).

Required Downtime

The firmware upgrade takes approximately 40 minutes to complete. During this time the Cisco Secure Endpoint functionality will not be available.

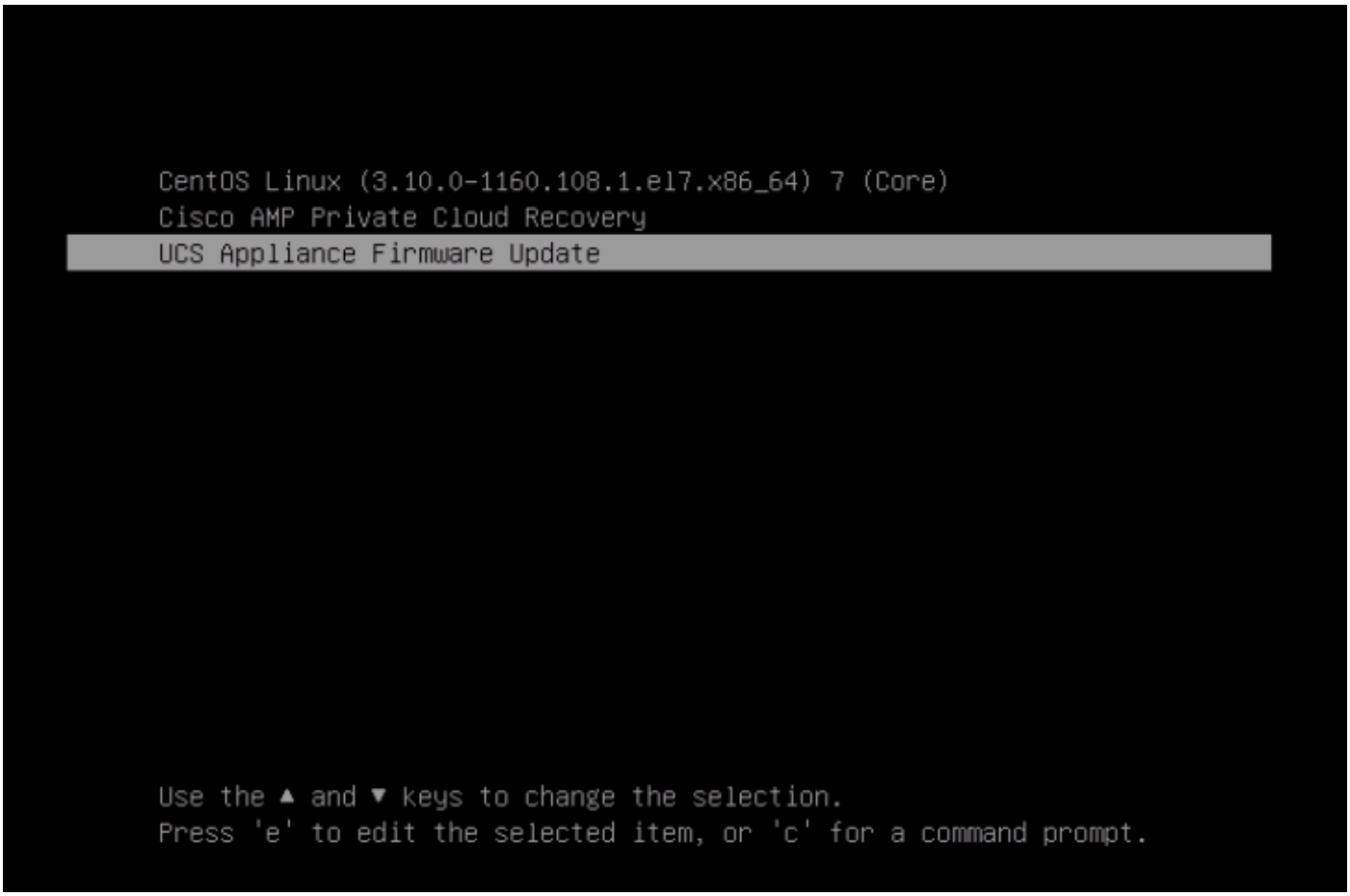
After the firmware upgrade is complete, the UCS appliance will be rebooted. This can take another 10 minutes.

Total downtime is approximately 50 minutes.

Firmware Upgrade Steps

Proxy or Connected Mode

1. Run the following commands on the appliance command line (either through SSH or CIMC KVM): *yum install -y ucs-firmware*
2. In your web browser, log into the CIMC web UI of the appliance and open the KVM console.
3. Reboot the appliance with (either from SSH or the CIMC KVM console): *amp-ctl reboot*
4. In the CIMC KVM console, wait for the appliance to reboot. In the boot loader menu, a new "UCS Appliance Firmware Update" menu item will be available (see screenshot below).
5. The boot loader will wait a couple of seconds before booting the normal appliance. Use the down arrow to select "UCS Appliance Firmware Update" and press enter.
6. The appliance will boot into the firmware updater, update the firmware and reboot the appliance.
7. The CIMC may log you out during this process.



Airgap Mode

1. Create a new update ISO using amp-sync.
2. Mount the update ISO as for a normal appliance update.
3. Run the following commands on the appliance command line (either through SSH or CIMC KVM): *yum install -y ucs-firmware*
4. In your web browser, log into the CIMC web UI of the appliance and open the KVM console.
5. Reboot the appliance with (either from SSH or the CIMC KVM console): *amp-ctl reboot*
6. In the CIMC KVM console, wait for the appliance to reboot. In the boot loader menu, a new "UCS Appliance Firmware Update" menu item will be available (see screenshot above).
7. The boot loader will wait a couple of seconds before booting the normal appliance. Use the down arrow to select "UCS Appliance Firmware Update" and press enter.
8. The appliance will boot into the firmware updater, update the firmware and reboot the appliance.
9. The CIMC may log you out during this process.

Verification Steps

1. In the CIMC web UI, go to the menu: Admin -> Firmware Management (see example screenshot below).
2. The BMC version should be 4.3(2.240009).

Firmware Management

Update | Activate

	Component	Running Version	Backup Version	Bootloader Version	Status	Progress in %
☐	BMC	4.3(2.240009)	4.2(3e)	4.3(2.240009)	Completed Successfully	
☐	BIOS	C240M6.4.3.2e.0_EDR	C240M6.4.3.2e.0_EDR	N/A	Completed Successfully	
☐	Cisco 12G SAS RAID Controller with 4GB FBWC (28 Drives)	52.20.0-4523	N/A	N/A	N/A	N/A
☐	SASEXP1	65160900	65160700	65160700	None	