Actualización de firmware de Cisco Secure Endpoint Private Cloud para CVE-2024-20356

Contenido

Introducción

La corrección de CVE-2024-20356 requiere una actualización del firmware CIMC para el dispositivo Cisco Secure Endpoint Private Cloud. En este artículo se describe el proceso de actualización del firmware de un dispositivo UCS de nube privada.

Prerequisites

- Appliance UCS de nube privada de terminal seguro con nube privada versión 3.9.x o posterior.
- Acceso a la interfaz de usuario web del appliance UCS de nube privada CIMC (incluido el acceso al KVM basado en Web).

Tiempo de inactividad requerido

La actualización del firmware tarda aproximadamente 40 minutos. Durante este tiempo, la funcionalidad de Cisco Secure Endpoint no estará disponible.

Una vez completada la actualización del firmware, se reiniciará el equipo UCS. Esto puede tardar otros 10 minutos.

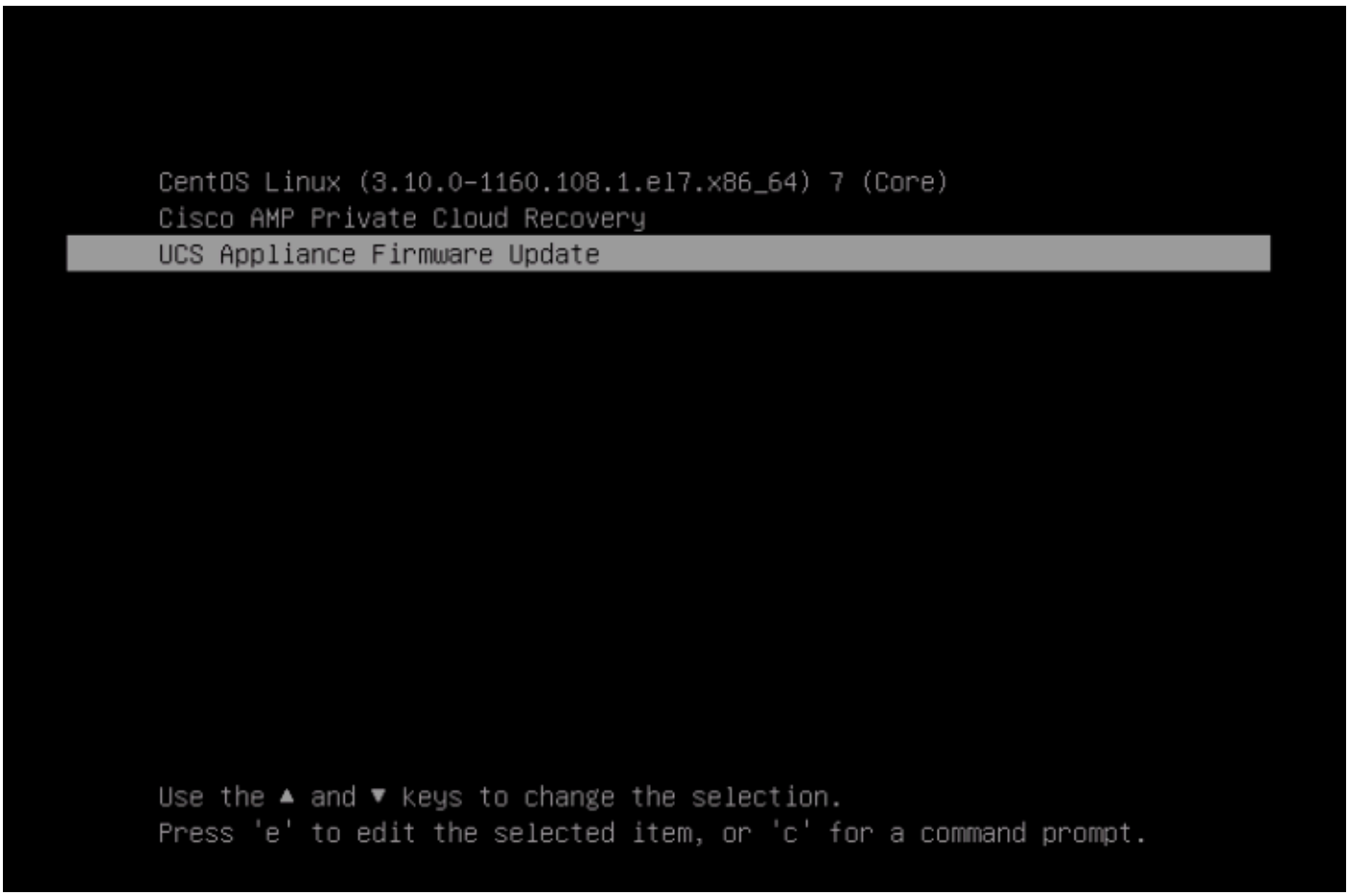
El tiempo de inactividad total es de aproximadamente 50 minutos.

Pasos de actualización del firmware

Proxy o modo conectado

1. Ejecute los siguientes comandos en la línea de comandos del equipo (ya sea mediante SSH o CIMC KVM): yum install -y ucs-firmware
2. En el explorador Web, inicie sesión en la interfaz de usuario Web de CIMC del equipo y abra la consola KVM.
3. Reinicie el equipo con (desde SSH o desde la consola KVM CIMC): amp-ctl reboot
4. En la consola KVM CIMC, espere a que se reinicie el equipo. En el menú del cargador de arranque, aparecerá un nuevo elemento de menú "UCS Appliance Firmware Update" (Actualización del firmware del equipo UCS) (consulte la captura de pantalla siguiente).
5. El cargador de arranque esperará un par de segundos antes de arrancar el dispositivo normal. Utilice la flecha hacia abajo para seleccionar "UCS Appliance Firmware Update" (Actualización del firmware del equipo UCS) y pulse Intro.

6. El equipo se iniciará en el actualizador de firmware, actualizará el firmware y reiniciará el equipo.
7. Es posible que el CIMC cierre su sesión durante este proceso.



Modo Airgap

1. Cree un nuevo ISO de actualización mediante amp-sync.
2. Monte el ISO de actualización como si se tratase de una actualización normal del dispositivo.
3. Ejecute los siguientes comandos en la línea de comandos del equipo (ya sea mediante SSH o CIMC KVM): yum install -y ucs-firmware
4. En el explorador Web, inicie sesión en la interfaz de usuario Web de CIMC del equipo y abra la consola KVM.
5. Reinicie el equipo con (desde SSH o desde la consola KVM CIMC): amp-ctl reboot
6. En la consola KVM CIMC, espere a que se reinicie el equipo. En el menú del cargador de arranque, aparecerá un nuevo elemento de menú "UCS Appliance Firmware Update" (Actualización del firmware del equipo UCS) (consulte la captura de pantalla anterior).
7. El cargador de arranque esperará un par de segundos antes de arrancar el dispositivo normal. Utilice la flecha hacia abajo para seleccionar "UCS Appliance Firmware Update" (Actualización del firmware del equipo UCS) y pulse Intro.
8. El equipo se iniciará en el actualizador de firmware, actualizará el firmware y reiniciará el equipo.
9. Es posible que el CIMC cierre su sesión durante este proceso.

Pasos de verificación

1. En la interfaz de usuario web de CIMC, vaya al menú: Admin -> Firmware Management (consulte la captura de pantalla de ejemplo siguiente).
2. La versión de BMC debe ser 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	

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).