

# Mise à niveau du micrologiciel du cloud privé Cisco Secure Endpoint pour CVE-2024-20356

## Table des matières

---

---

### Introduction

La correction du CVE-2024-20356 nécessite une mise à jour du micrologiciel CIMC pour l'appliance de cloud privé Cisco Secure Endpoint. Cet article décrit le processus de mise à niveau du micrologiciel d'une appliance de cloud privé UCS.

### Conditions préalables

- Appliance UCS de cloud privé pour terminaux sécurisés avec cloud privé version 3.9.x ou ultérieure.
- Accès à l'interface utilisateur Web CIMC de l'appliance de cloud privé UCS (y compris l'accès au KVM basé sur le Web).

### Temps d'arrêt requis

La mise à niveau du micrologiciel prend environ 40 minutes. Pendant ce temps, la fonctionnalité Cisco Secure Endpoint ne sera pas disponible.

Une fois la mise à niveau du micrologiciel terminée, le périphérique UCS redémarre. Cela peut prendre encore 10 minutes.

Le temps d'arrêt total est d'environ 50 minutes.

### Étapes de mise à niveau du microprogramme

#### Proxy ou mode connecté

1. Exécutez les commandes suivantes sur la ligne de commande du matériel (via SSH ou CIMC KVM) : `yum install -y ucs-firmware`
2. Dans votre navigateur Web, connectez-vous à l'interface utilisateur Web CIMC du matériel et ouvrez la console KVM.
3. Redémarrez le matériel avec (à partir de SSH ou de la console KVM CIMC) : `amp-ctl reboot`
4. Dans la console KVM CIMC, attendez le redémarrage du matériel. Dans le menu du chargeur de démarrage, un nouvel élément de menu « UCS Appliance Firmware Update » sera disponible (voir capture d'écran ci-dessous).
5. Le chargeur de démarrage attend quelques secondes avant de démarrer l'appliance normale. Utilisez la flèche vers le bas pour sélectionner « UCS Appliance Firmware Update

- » et appuyez sur Entrée.
6. Le matériel démarre dans le programme de mise à jour du micrologiciel, met à jour le micrologiciel et redémarre le matériel.
  7. Le CIMC peut vous déconnecter au cours de ce processus.



```
CentOS Linux (3.10.0-1160.108.1.el7.x86_64) 7 (Core)
Cisco AMP Private Cloud Recovery
UCS Appliance Firmware Update
```

Use the ▲ and ▼ keys to change the selection.  
Press 'e' to edit the selected item, or 'c' for a command prompt.

## Mode D'Entrefer

1. Créez une nouvelle mise à jour ISO en utilisant amp-sync.
2. Montez l'ISO de mise à jour comme pour une mise à jour normale de l'appliance.
3. Exécutez les commandes suivantes sur la ligne de commande du matériel (via SSH ou CIMC KVM) : `yum install -y ucs-firmware`
4. Dans votre navigateur Web, connectez-vous à l'interface utilisateur Web CIMC du matériel et ouvrez la console KVM.
5. Redémarrez le matériel avec (à partir de SSH ou de la console KVM CIMC) : `amp-ctl reboot`
6. Dans la console KVM CIMC, attendez le redémarrage du matériel. Dans le menu du chargeur de démarrage, un nouvel élément de menu « UCS Appliance Firmware Update » est disponible (voir capture d'écran ci-dessus).
7. Le chargeur de démarrage attend quelques secondes avant de démarrer l'appliance normale. Utilisez la flèche vers le bas pour sélectionner « UCS Appliance Firmware Update » et appuyez sur Entrée.
8. Le matériel démarre dans le programme de mise à jour du micrologiciel, met à jour le micrologiciel et redémarre le matériel.
9. Le CIMC peut vous déconnecter au cours de ce processus.

# Étapes de vérification

1. Dans l'interface utilisateur Web de CIMC, accédez au menu Admin -> Firmware Management (voir l'exemple de capture d'écran ci-dessous).
2. La version BMC doit être 4.3(2.240009).

## Firmware Management

<input type="button" value="Update"/> <input type="button" value="Activate"/>						
<input type="checkbox"/>	Component	Running Version	Backup Version	Bootloader Version	Status	Progress in %
<input type="checkbox"/>	BMC	4.3(2.240009)	4.2(3e)	4.3(2.240009)	Completed Successfully	
<input type="checkbox"/>	BIOS	C240M6.4.3.2e.0_EDR	C240M6.4.3.2e.0_EDR	N/A	Completed Successfully	
<input type="checkbox"/>	Cisco 12G SAS RAID Controller with 4GB FBWC (28 Drives)	52.20.0-4523	N/A	N/A	N/A	N/A
<input type="checkbox"/>	SASEXP1	65160900	65160700	65160700	None	

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.