# Mise à niveau du micrologiciel du cloud privé Cisco Secure Endpoint

## Table des matières


Introduction

Conditions préalables

Temps d'arrêt requis

Étapes de mise à niveau du microprogramme

- Proxy ou mode connecté
- Mode D'Entrefer
- Vérification supplémentaire

Instructions héritées (pour la correction de CVE-2024-20356)

- Étapes de mise à niveau du microprogramme
- Proxy ou mode connecté
- Mode D'Entrefer
- Étapes de vérification


## Introduction

Cet article décrit le processus de mise à niveau du micrologiciel d'une appliance Cisco Secure Endpoint Private Cloud UCS. La documentation précédente relative à la correction du CVE-2024-20356 a été déplacée vers une section Instructions héritées.

## Conditions préalables

- Appliance UCS de cloud privé pour terminaux sécurisés avec cloud privé version 4.2.5 ou ultérieure.
  - Les instructions héritées s'appliquent à un cloud privé avec les versions 3.9.x à 4.2.4.
- Accès à l'interface utilisateur Web CIMC de l'appliance de cloud privé UCS.

### Temps d'arrêt requis

La mise à niveau du RPM via Opadmin prend environ 10 minutes. La mise à niveau du micrologiciel elle-même prend environ 40 minutes. Pendant ce temps, la fonctionnalité Cisco Secure Endpoint ne sera pas disponible.

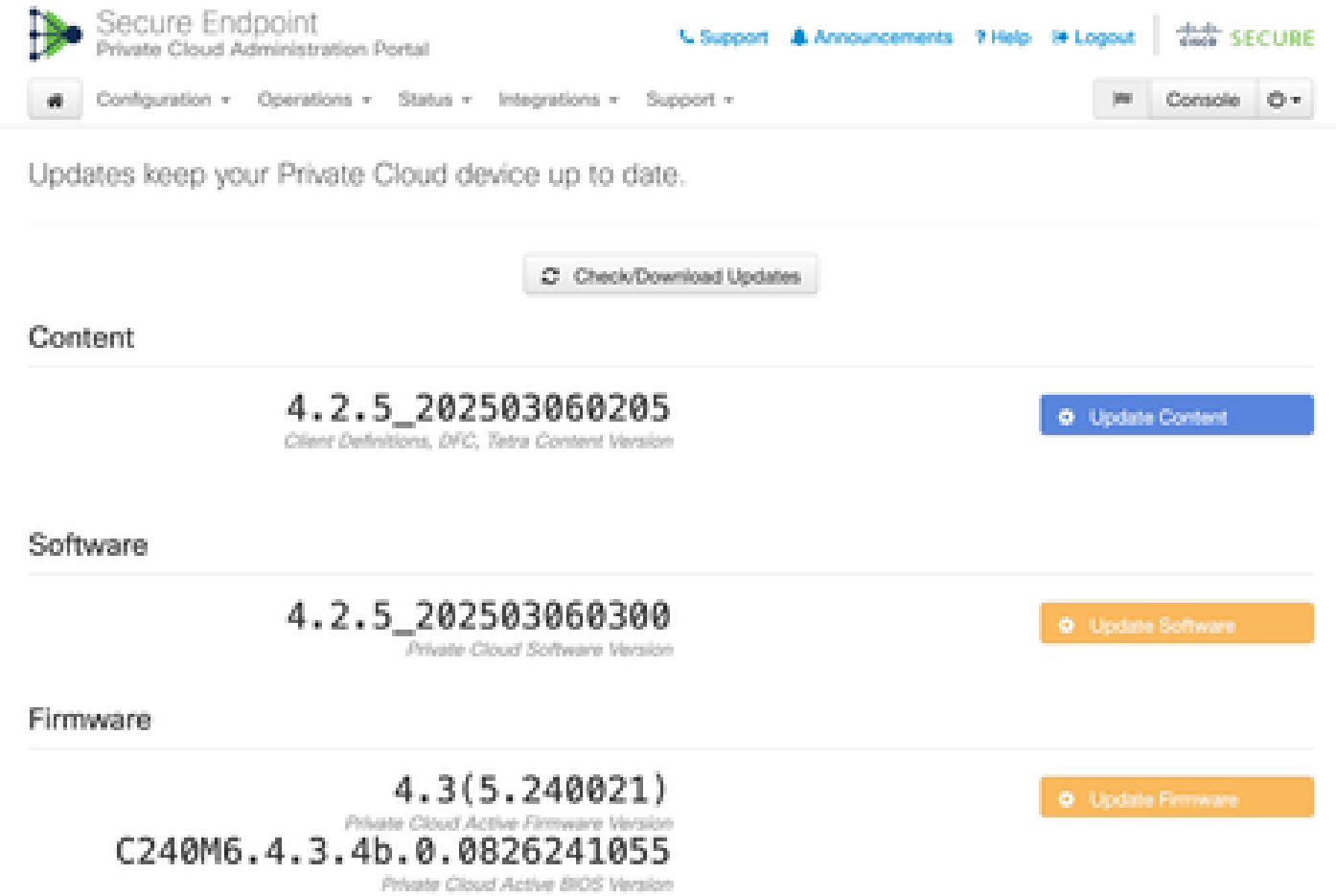
Une fois la mise à niveau du micrologiciel terminée, le périphérique UCS redémarre. Cela peut prendre encore 10 minutes.

Le temps d'arrêt total est d'environ 60 minutes.

## Étapes de mise à niveau du microprogramme

## Proxy ou mode connecté

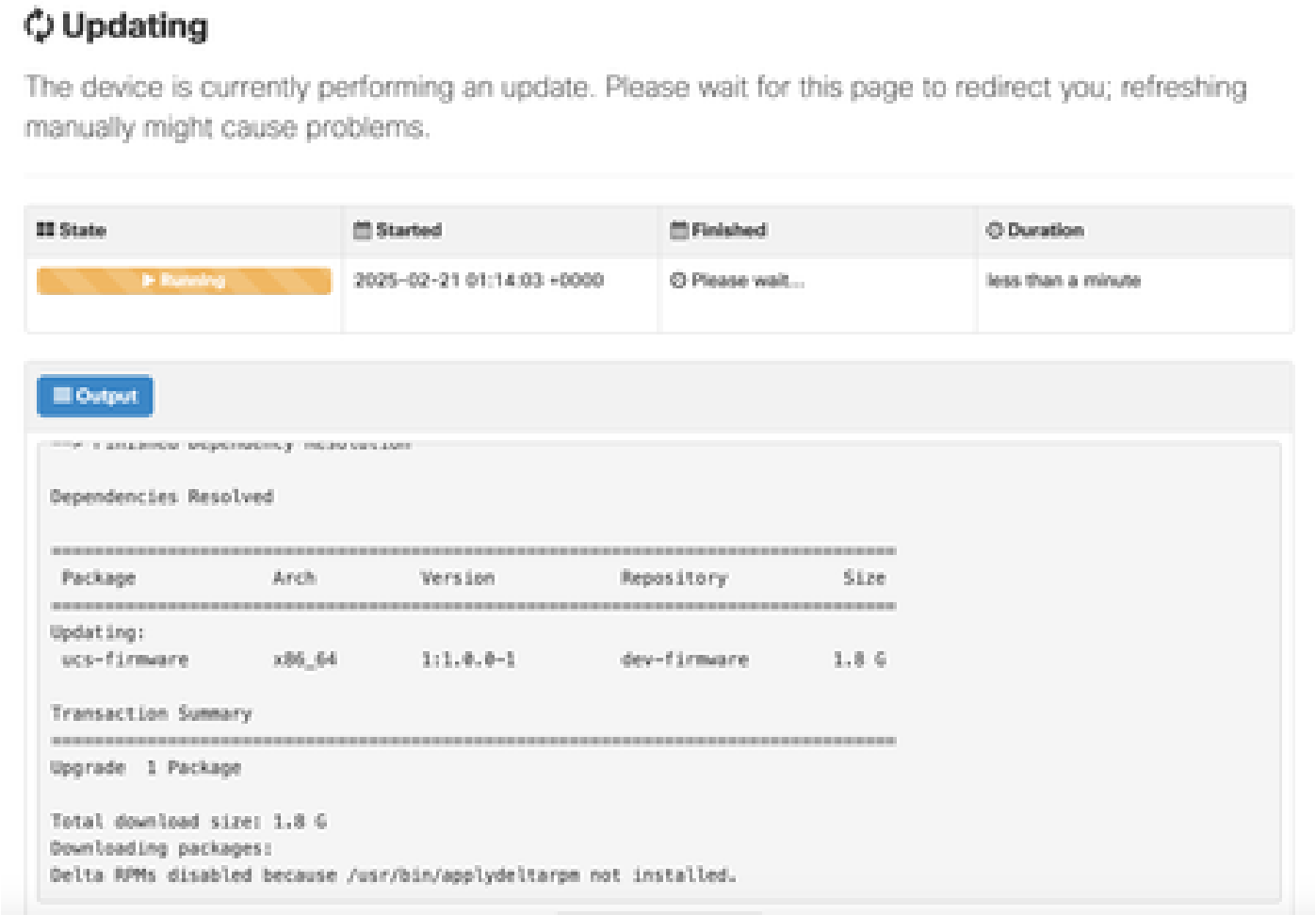
1. Accédez à Operations > Updates, comme indiqué dans l'image.




2. L'appliance doit rechercher chaque jour de nouvelles mises à jour du micrologiciel. Si elle n'a pas encore été cochée et marquée comme disponible, cliquez sur le bouton Check/Download Updates.

3. Cliquez sur le bouton Update Firmware, comme illustré dans l'image.

4. La mise à jour du micrologiciel commence, comme indiqué dans l'image.

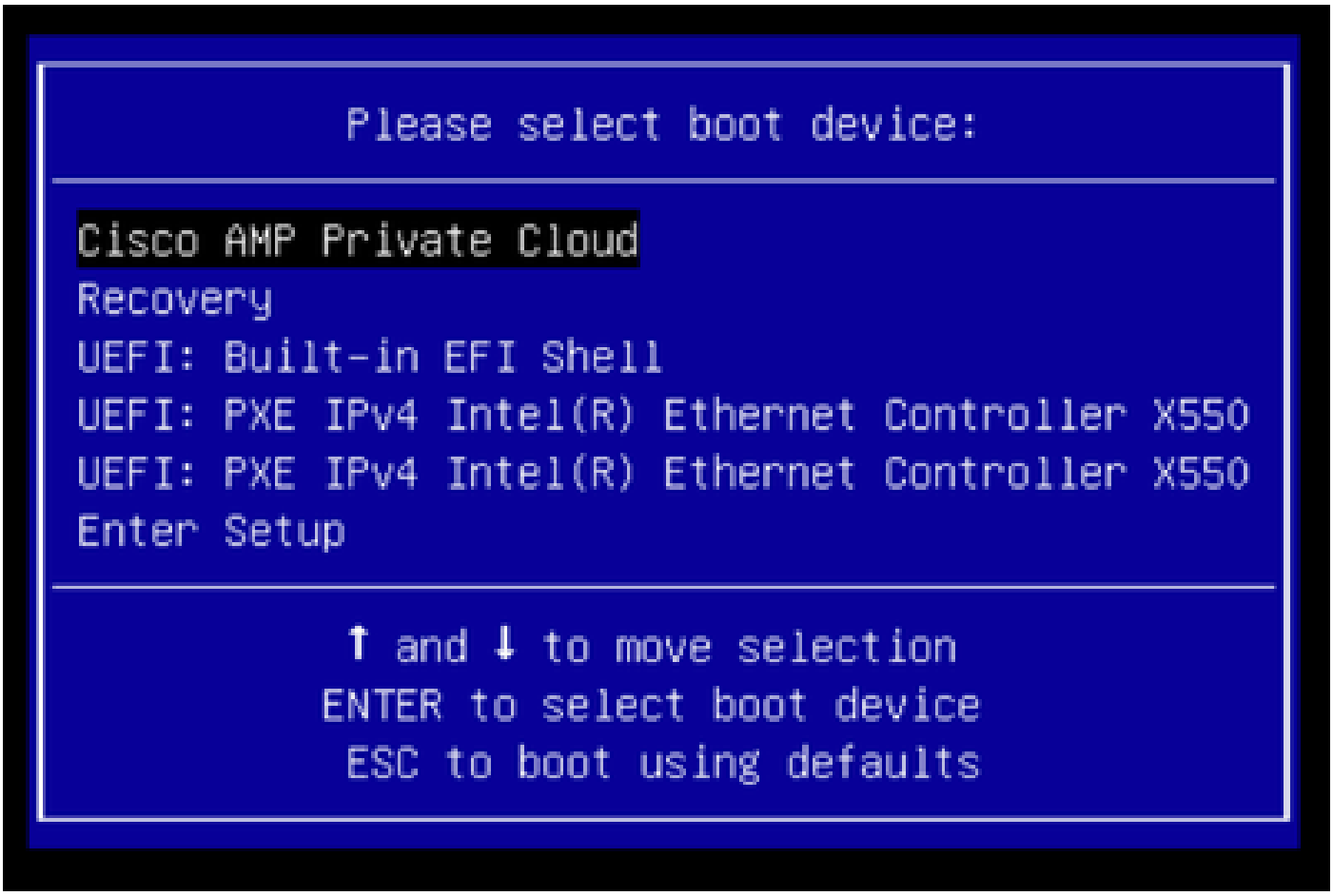



5. Attendez la fin de la mise à jour. Une fois cette opération effectuée, nous devons toujours redémarrer le matériel et terminer la mise à jour du micrologiciel. Pour ce faire, procédez comme suit :

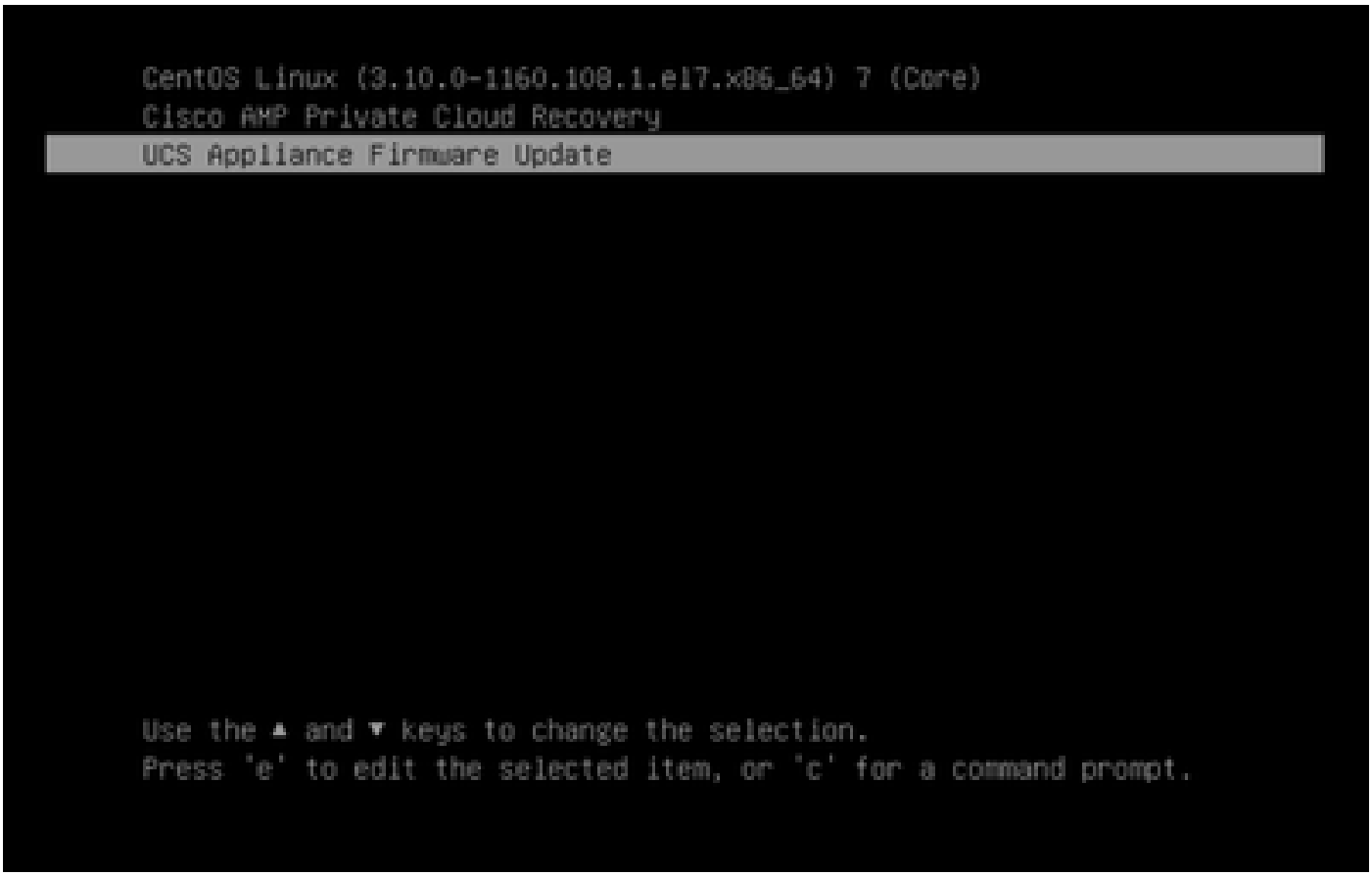
6. Dans votre navigateur Web, connectez-vous à l'interface utilisateur Web CIMC du matériel et ouvrez la console KVM.

7. Redémarrez le matériel avec (à partir de SSH ou de la console KVM CIMC) : amp-ctl reboot

8. Dans la console KVM CIMC, attendez le redémarrage du matériel. Dans le menu du chargeur de démarrage, utilisez la flèche vers le bas pour sélectionner Cisco AMP Private Cloud :




9. Le chargeur de démarrage attend quelques secondes avant de démarrer l'appareil normal. Utilisez la flèche vers le bas pour sélectionner UCS Appliance Firmware Update et appuyez sur Entrée :




10. Le matériel démarre dans le programme de mise à jour du micrologiciel, met à jour le micrologiciel et redémarre le matériel.

11. Le CIMC peut vous déconnecter au cours de ce processus.

## Mode D'Entrefer

1. Téléchargez une nouvelle version d'amp-sync. Dans la version 4.2.5, une nouvelle version d'amp-sync est disponible, qui récupère les mises à jour du microprogramme en même temps que le contenu et les mises à jour logicielles.
2. Créez une nouvelle mise à jour ISO en utilisant amp-sync.
3. Montez l'ISO de mise à jour comme pour une mise à jour normale de l'appliance.
4. Accédez à Opérations > Mises à jour.
5. Cliquez sur le bouton Vérifier la mise à jour ISO.
6. Une fois les mises à jour disponibles, cliquez sur le bouton Update Firmware.

7. Attendez la fin de la mise à jour. Une fois cette opération effectuée, nous devons toujours redémarrer le matériel et terminer la mise à jour du micrologiciel. Pour ce faire, procédez comme suit :

8. Dans votre navigateur Web, connectez-vous à l'interface utilisateur Web CIMC du matériel et ouvrez la console KVM.

9. Redémarrez le matériel avec (à partir de SSH ou de la console KVM CIMC) : amp-ctl reboot

10. Dans la console KVM CIMC, attendez le redémarrage du matériel. Dans le menu du

chargeur de démarrage, utilisez la flèche vers le bas pour sélectionner Cisco AMP Private Cloud.

11. 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.

12. Le matériel démarre dans le programme de mise à jour du micrologiciel, met à jour le micrologiciel et redémarre le matériel.

13. Le CIMC peut vous déconnecter au cours de ce processus.

### Vérification supplémentaire

1. Accédez à Opérations > Mises à jour.
2. Vérifiez que les versions actives du micrologiciel et du BIOS ont été mises à jour.
3. Vous pouvez également accéder au menu de l'interface utilisateur Web de CIMC : Admin -> Firmware Management (Gestion du micrologiciel), comme illustré dans l'image.

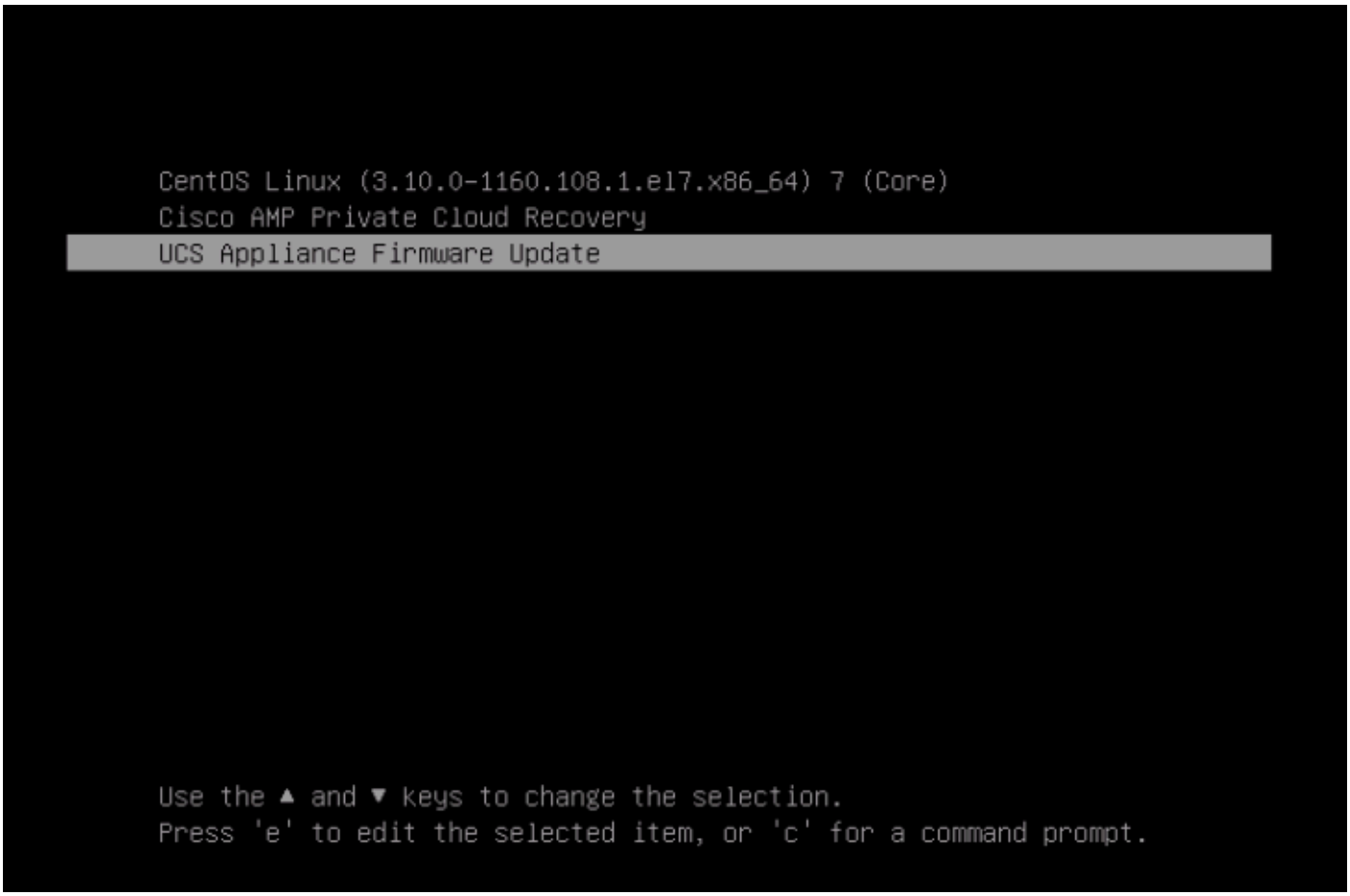
## Instructions héritées (pour la correction de CVE-2024-20356)

Ces instructions peuvent être utilisées pour les appliances de cloud privé avec les versions 3.9.x jusqu'à 4.2.4.

### 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.




## 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 capture d'écran ci-dessous).

2. La version BMC doit être 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 | |

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.