

Atualização do firmware da nuvem privada do Cisco Secure Endpoint para CVE-2024-20356

Contents

Introdução

A correção do CVE-2024-20356 requer uma atualização do firmware do CIMC para o dispositivo Cisco Secure Endpoint Private Cloud. Este artigo descreve o processo de atualização do firmware de um dispositivo UCS de nuvem privada.

Pré-requisitos

- Secure Endpoint Private Cloud UCS Appliance com Private Cloud versão 3.9.x ou superior.
- Acesso à interface do usuário da Web do CIMC do dispositivo UCS de nuvem privada (incluindo acesso ao KVM baseado na Web).

Tempo de inatividade necessário

A atualização do firmware leva aproximadamente 40 minutos para ser concluída. Durante esse período, a funcionalidade do Cisco Secure Endpoint não estará disponível.

Após a conclusão da atualização do firmware, o dispositivo UCS será reinicializado. Isso pode levar mais 10 minutos.

O tempo de inatividade total é de aproximadamente 50 minutos.

Etapas de atualização do firmware

Modo Proxy ou Conectado

1. Execute os seguintes comandos na linha de comando do equipamento (através do SSH ou do CIMC KVM): `yum install -y ucs-firmware`
2. No navegador da Web, faça login na interface do usuário da Web do CIMC do equipamento e abra o console KVM.
3. Reinicialize o equipamento com (do SSH ou do console KVM do CIMC): `reinicialização amp-ctl`
4. No console KVM do CIMC, aguarde a reinicialização do equipamento. No menu do carregador de inicialização, um novo item do menu "Atualização do firmware do dispositivo UCS" estará disponível (veja a captura de tela abaixo).
5. O carregador de inicialização aguardará alguns segundos antes de inicializar o equipamento normal. Use a seta para baixo para selecionar "Atualização do firmware do dispositivo UCS"

- e pressione Enter.
6. O equipamento será inicializado no atualizador de firmware, atualizará o firmware e reinicializará o equipamento.
 7. O CIMC pode desconectá-lo durante esse processo.

```
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.
```

Modo Airgap

1. Crie um novo ISO de atualização usando amp-sync.
2. Monte o ISO de atualização como para uma atualização normal do equipamento.
3. Execute os seguintes comandos na linha de comando do equipamento (através do SSH ou do CIMC KVM): `yum install -y ucs-firmware`
4. No navegador da Web, faça login na interface do usuário da Web do CIMC do equipamento e abra o console KVM.
5. Reinicialize o equipamento com (do SSH ou do console KVM do CIMC): `reinicialização amp-ctl`
6. No console KVM do CIMC, aguarde a reinicialização do equipamento. No menu do carregador de inicialização, um novo item do menu "Atualização do firmware do dispositivo UCS" estará disponível (veja a captura de tela acima).
7. O carregador de inicialização aguardará alguns segundos antes de inicializar o equipamento normal. Use a seta para baixo para selecionar "Atualização do firmware do dispositivo UCS" e pressione Enter.
8. O equipamento será inicializado no atualizador de firmware, atualizará o firmware e reinicializará o equipamento.

9. O CIMC pode desconectá-lo durante esse processo.

Etapas de verificação

1. Na IU da Web do CIMC, vá para o menu: Admin -> Firmware Management (veja a captura de tela abaixo).
2. A versão do BMC deve ser 4.3(2.240009).

Firmware Management

		Update		Activate	
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	

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.