如何使用EFI Shell將安全惡意軟體分析裝置引導 至恢復模式並將恢復模式新增到引導選項

目錄

<u>簡介</u> <u>問題</u> <u>解決方案</u> <u>EFI外殼</u> 將恢復模式新增到引導選項

簡介

本文檔介紹如何使用EFI Shell將Secure Malware Analytics®裝置引導至恢復模式並將恢復模式新增 到引導選項的步驟。

問題

您可以看到如下圖所示,BIOS視窗中未顯示恢復模式:

Please select boot device:

Appliance UEFI: Built-in EFI Shell UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection Enter Setup

> ↑ and ↓ to move selection ENTER to select boot device ESC to boot using defaults

在此案例中,為了能夠引導進入恢復模式,必須使用下一節中介紹的步驟。

解決方案

EFI外殼

步驟1.將KVM介面卡連線到外部顯示器和鍵盤,並將其插入裝置前面的KVM埠。如果CIMC可用且 已配置,則可以使用遠端KVM。

步驟3.在BIOS視窗中按F6獲取可能的引導目標清單。



Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration, <F12> Network Boot

Bios Version : C220M4.4.0.2d.0.0627191019 Platform ID : C220M4

Cisco IMC IPv4 Address : Cisco IMC MAC Address :

Processor(s) Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz Total Memory = 512 GB Effective Memory = 512 GB Memory Operating Speed 2400 Mhz Entering boot selection menu...

步驟4.選擇UEFI:內建EFI外殼。

Please select boot device:

Appliance UEFI: Built-in EFI Shell UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection Enter Setup

> ↑ and ↓ to move selection ENTER to select boot device ESC to boot using defaults

步驟5.在此之後,請在啟動指令碼完成之前按ESC以移入EFI Shell。

步驟6.可用檔案系統的清單。

UEFI Interactive Shell v2.0. UEFI v2.40 (American Megatrends, 0x0005000B). Revision 1.02
Manning table
fs0: Alias(s):HD29a0b:;blk1:
PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(1,GPT,7303FEC6-7E81-4D88-961C-AE562681960F,0x800,0x4
00000)
fs1: Alias(s):HD29b0b:;blk5:
PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)/HD(1,GPT,C65AF6B6-C149-4184-B744-EB15CD038D5B,0x800,0x4
00000)
blk0: Alias(s):
PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)
blk4: Alias(s):
PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)
blk2: Alias(s):
PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctr1(0x0)/Scsi(0x0,0x0)/HD(2,GPT,900A83C7-D4F4-44C3-B6D3-35D2DCC6249F,0x400800,
0x400000)
blk3: Alias(s):
PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(3,GPT,D5A6A81E-85F9-4648-9277-3E4A89B43D65,0x800800,
0xD5A6FDF)
blk6: Alias(s):
PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)/HD(2,GPT,ED9A0467-38FD-4DCF-A409-057CEC64FA1E,0x400800,
0x289A8CFDF)
Press ESC in 5 seconds to skip startup.nsh or any other key to continue.
Shell>

步驟7。此時,您需要找到位於其中一個檔案系統中的Recovery目錄。

步驟8.導航到該目錄。

Shell> fs1:				
fs1:∖> dir				
Directory of	f: fs1:∖			
03/16/2022	17:12		31,736	meta_contents.tar.xz
10/26/2020	11:29		149	startup.nsh
12/21/2016	23:42 KD	IR>	4,096	
04/30/2021	08:28	836,	030,464	recovery.rosfs
3	File(s)	836,062,34	9 bytes	
1	Dir(s)			
fs1:\> cd e	fi			
fs1:\efi\> (dir			
Directory of	f: fs1:∖e	fi\		
12/21/2016	23:42 KD	IR>	4,096	
12/21/2016	23:42 KD	IR>	0	
04/30/2021	08:28 <d< td=""><td>IR></td><td>4,096</td><td></td></d<>	IR>	4,096	
0	File(s)	Q) bytes	
3	Dir(s)			
fs1:\efi\> (d Recover	ry		
fs1:\efi\Red	covery\> (dir		
Directory of	f: fs1:∖e	fi∖Recovery	N .	
12/21/2016	23:42 <d< td=""><td>IR></td><td>4,096</td><td></td></d<>	IR>	4,096	
12/21/2016	23:42 <d< td=""><td>IR></td><td>4,096</td><td></td></d<>	IR>	4,096	
04/30/2021	08:28	18,2	55,144	boot.efi
1	File(s)	18,255,144	bytes	
2	Dir(s)			

步驟10.裝置啟動至恢復模式。

>>		
>>		
>>	help	
	COMMANDS:	
	configure	showlset: View or modify configuration variables
	coms	listeninglopentall: Show open connections
	destroy-data	Reset appliance to be a target for the restore process
	exit	Exit tgsh.
	graphql	Following content until the next empty line is treated as a GraphQL query to run
	halt	Halt appliance
	help	List available commands, or 'help COMMAND' for details.
	netconfig	Update configured network settings
	netconfig-apply	Modify active network configuration to match saved settings
	netinfo	routes firewall addrs stats: Show network configuration and status
	opadnin	importIcheck: Sync from, or validate, new configuration format
	passud	Change password for this account
	ping	ping [-c count] [-[interface] host: ping a remote host
	poweroff	Fouer off appliance
	reboot	Reboot appliance
	reconfigure	simple/with-reinstall: Mondestructively rerun configuration in single-user mode, with or without precedin
a i	reinstall	
	service	tstatusistartistopirestarti (suc-name): loggie inreatorio services
	support-mode	statusistariistop: loggie support mode
	traceroute	Determine the path used to a network location
	Jersion	shows appriance version
- 77		

將恢復模式新增到引導選項

步驟1.將KVM介面卡連線到外部顯示器和鍵盤,並將其插入裝置前面的KVM埠。如果CIMC可用且 已配置,則可以使用遠端KVM。

步驟2.重新啟動裝置。

步驟3.在BIOS視窗中按F6獲取可能的引導目標清單。

ıılııılıı cısco
Press <f2> Setup, <f6> Boot Menu, <f7> Diagnostics, <f8>Cisco IMC Configuration, <f12> Network Boot</f12></f8></f7></f6></f2>
Bios Version : C220M4.4.0.2d.0.0627191019 Platform ID : C220M4
Cisco IMC IPv4 Address : Cisco IMC MAC Address :
Processor(s) Intel(R) Xeon(R) CPU E5–2697 v4 0 2.30GHz Total Memory = 512 GB Effective Memory = 512 GB Memory Operating Speed 2400 Mhz Entering boot selection menu

步驟4.選擇**輸入設定**。

Please select boot device:

步驟5.導覽至Boot Options,滾動至底部,然後選擇Add New Boot Option。

Aptio Setup Utility Main Advanced Server	– Copyright (C) 2019 Americ Management Security Boot	can Megatrends, Inc. Options Save & Exit
Setup Prompt Timeout Check controllers health status	3 [Enabled]	Add a new EFI boot option to the boot order
UEFI Boot Options	[Enabled]	
Boot Option Priorities Boot Option #1 Boot Option #2	[Appliance] [UEFI: Built-in EFI Shell]	
Boot Option #3	[UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection]	↔ Select Screen ↑↓ Select Item Enter Select Field
Boot Option #4	[UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection]	+/- Change Value F1 General Help F9 BIOS Defaults F10 Save & Exit
► Add New Boot Option ► Delete Boot Option	•	ESC Exit

步驟6.選擇Add boot option,然後鍵入Recovery。

Aptio Setup Utility – Copyright (C) 2019 Americ Boot	an Megatrends, Inc. Options
Add New Boot Option Add boot option Path for boot option Boot option File Path Create Add boot option Recovery_	Specify name for new boot option
	✤ Select Screen ↑↓ Select Item Enter Select Field +/- Change Value F1 General Help F9 BIOS Defaults F10 Save & Exit ESC Exit

步驟7.選擇Path for boot選項並</mark>選擇正確的File System。

Aptio Setup Utility – Copyright (C) 2019 Ameri Boot	can Megatrends, Inc. Options	
Add New Boot Option Add boot option Path for boot option Boot option File Path	Enter the path to the boot option in the format fsx:\path\filename.efi	
Select a File System		
PCI(2 2)\PCI(0 0)\DevicePath(Type 1, SubType 5)SCSI(0,0)\HD(Part1,Sig7303f PCI(2 2)\PCI(0 0)\DevicePath(Type 1, SubType 5)SCSI(1,0)\HD(Part1,Sigc65af		
	†↓ Select Item Enter Select Field +/- Change Value F1 General Help F9 BIOS Defaults F10 Save & Exit ESC Exit	

步驟8.選**擇<efi>、<Recovery>和<boot.efi>**。





步驟9.選擇Create。

Aptio Setup Utility	y – Copyright (C) 2019 Amerio Boot	can Megatrends, Inc. Options
Add New Boot Option		Creates the newly formed boot option
Add boot option Path for boot option	Recovery	
Boot option File Path Create	∖efi\Recovery\boot.efi	
		++ Select Screen
		↑↓ Select Item
		Enter Select Field
		+/- Change Value
		F1 General Help
		F9 BIOS Defaults
		FIO SAVE & EXIC ESC Evit
		LOO LAIT

步驟10.建立新引導選項。



步驟12.使用+/ — 按#2將Recovery選項放在適當的位置。

Aptio Setup Utility Main Advanced Server	– Copyright (C) 2019 Ameri Management Security Boot	can Megatrends, Inc. Options Save & Exit
Policy type in use: Boot Configuration Setup Prompt Timeout Check controllers health status	Boot Order Table	Sets the system boot order
UEFI Boot Options Boot Option Priorities	[Enabled]	
Boot Option #1	[Appliance]	
Boot Option #2	[Recovery]	++ Select Screen
Boot Option #3	[UEFI: Built-in EFI Shell]	†↓ Select Item Enter Select Field
Boot Option #4	[UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection]	+/- Change Value F1 General Help F9 BIOS Defaults
Boot Option #5	[UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection]	F10 Save & Exit ESC Exit

步驟13.導覽至Save & Exit,然後選擇Save Changes and Exit。

Aptio Setup Utility – Copyright (C) 2019 Americ	can Megatrends, Inc.
Main Advanced Server Management Security Boot	Options Save & Exit
Save Changes and Exit	Exit system setup after
Discard Changes and Exit	saving the changes.
Save Options Save Changes Discard Changes	
Restore Defaults Save as User Defaults Restore User Defaults Load Manufacturing Default Values	→+ Select Screen
Boot Override Appliance Recovery	↑↓ Select Item Enter Select Field +/- Change Value F1 General Help F8 BIOS Defaulte
UEFI: Built-In EFI Shell	F9 Blos Defaults
UEFI: IP4 0100 Intel(R) I350 Gigabit Network	F10 Save & Exit
Connection	ESC Exit

步驟14.確認更改。



步驟15.裝置正常啟動。

有關詳細資訊,請參閱安全惡意軟體分析裝置管理指南。