如何使用EFI外壳将安全恶意软件分析设备引导到 恢复模式并向引导选项添加恢复模式

目录

<u>简介</u> <u>问题</u> <u>解决方案</u> <u>EFI外壳</u> <u>将恢复模式添加到引导选项</u>

简介

本文档介绍如何使用EFI外壳将安全恶意软件分析®设备引导到恢复模式以及将恢复模式添加到引导 选项的步骤。

问题

您将能够看到,如图所示,BIOS窗口中未显示恢复模式:

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

要在此场景中引导到恢复模式,我们必须使用下一节中介绍的步骤。

解决方案

EFI外壳

步骤1.将KVM适配器连接到外部显示器和键盘,并将其插入位于设备前面的KVM端口。如果 CIMC可用且已配置,则可以使用远程KVM。

步骤3.在BIOS窗口中按F6,查看可能的引导目标列表。



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...

步骤4.选择UEFI:内置EFI外壳。

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

步骤5.在启动脚本完成之后,按ESC键进入EFI Shell。

步骤6.可用文件系统的列表。

UEFI Interactive Shell v2.0. UEFI v2.40 (American Megatrends, 0x0005000B). Revision 1.02 Manaing table
fs0: Alias(s):HD29a0h::hlk1:
Priflox1,0027,0027,0027,0027,0027,0027,0027,002
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):
PciRaot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)
blk4: Alias(s):
PciRaat(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)
blk2: Alias(s):
PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(2,GPT,900A83C7-D4F4-44C3-B6D3-35D2DCC6249F,0x400800,
0x400000)
blk3: Alias(s):
PciRaat(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>

步骤7.此时,您需要找到位于其中一个文**件系**统中的"恢复"目录。

步骤8.导航到该目录。

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 ef	fi			
fs1:\efi\> (dir			
Directory of	f: fs1:∖e	fi\		
12/21/2016	23:42 KD	IR>	4,096	
12/21/2016	23:42 <d< td=""><td>IR></td><td>0</td><td></td></d<>	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)	0	bytes	
3	Dir(s)			
fs1:\efi\> (cd Recover	ry		
fs1:\efi\Red	covery\>	dir		
Directory of	f: fs1:∖e	fi\Recovery	\	
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)			

步骤10.设备引导到恢复模式。

>> >>		
>>	help COMMANDS:	
	configure	shoulest: Use on podify configuration variables
	come	Sinduraction of the or monthly configuration contacts
	dentrou-data	Denot analises to be a target for the restore response
	aestroy-aata	Reset appliance to be a target for the restore process
	exit	Exil ugsn.
	graphdi	rollowing content until the next empty line is treated as a Graphyl query to run
	halt	Halt appliance
	help	List available commands, or help cumminu 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
	opadmin	importIcheck: Sync from, or validate, new configuration format
	passud	Change password for this account
	ping	ping [-c count] [-I interface] host: ping a remote host
	poweroff	Power off appliance
	reboot	Reboot appliance
	reconfigure	simple/with-reinstall: Nondestructively rerun configuration in single-user mode, with or without precedin
g	reinstall	
	service	{status start stop restart} [suc-name]: Toggle ThreatGRID services
	support-mode	status start stop: Toggle support mode
	traceroute	Determine the path used to a network location
	version	Shows appliance version
>>		

将恢复模式添加到引导选项

步骤1.将KVM适配器连接到外部显示器和键盘,并将其插入位于设备前面的KVM端口。如果 CIMC可用且已配置,则可以使用远程KVM。

步骤2.重新启动设备。

步骤3.在BIOS窗口中按F6,查看可能的引导目标列表。

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 @ 2.30GHz Total Memory = 512 GB Effective Memory = 512 GB Memory Operating Speed 2400 Mhz Entering boot selection menu

步骤4.选择"**输入设置**"。

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

步骤5.导航至"**引导选**项",滚动到底部,然后选择"添加新引导选项"。

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	
Boot Option #3	Shell] [UEFI: IP4 0100 Intel(R) I350 Gigabit	↔ Select Screen †↓ Select Item
Boot Option #4	Network Connection] [UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection]	Enter Select Field +/– Change Value F1 General Help F9 BIOS Defaults
 Add New Boot Option Delete Boot Option 	•	F10 Save & Exit ESC Exit

步骤6.选择"添**加引导选项**"并键入"恢复"。

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

步骤7.选择Path for boot**选项,然后选**择适当的**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	

步骤8.选**择<efi>、<Recovery>和<boot.efi>**。





步骤9.选择"创**建"**。

Aptio Setup Utility) – Copyright (C) 2019 Ameri 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 f↓ Select Item Enter Select Field +/- Change Value F1 General Help
		F9 BIOS Defaults F10 Save & Exit ESC Exit

步骤10.创建新的引导选项。



步骤12.将"恢复"选项放在#2处,并带有+/ — 按钮。

Aptio Setup Utility Main Advanced Server	– Copyright (C) 2019 Americ 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	[Enabled]	
Boot Option Priorities		
Boot Option #1	[Appliance]	
Boot Option #2	[Recovery]	↔ Select Screen
Boot Option #3	[UEFI: Built-in EFI	↑↓ Select Item
Boot Option #4	Shell] [UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection]	Enter Select Field +/- 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

步骤13.导航至"保**存并退出",**然后选**择"保存更改并退出**"。

Aptio Setup Utility – Copyright (C) 2019 Ameria Main Advanced Server Management Security Boot	can Megatrends, Inc. Options Save & Exit
Save Changes and Exit Discard Changes and Exit	Exit system setup after 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
UEFI: Built-in EFI Shell UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection	F9 BIOS Defaults F10 Save & Exit ESC Exit

步骤14.确认更改。



步骤15.设备正常启动。

有关详细信息,请参阅<u>安全恶意软件分析设备管理指南</u>。