

升級到7.2.6期間針對CSCwi63113提供保護

目錄

[簡介](#)

[背景](#)

[升級前停用SNMP](#)

[FMC步驟：](#)

[第1步：登入到FMC](#)

[第2步：導航至Devices > Platform Settings](#)

[第3步：編輯與您的FTD裝置關聯的策略](#)

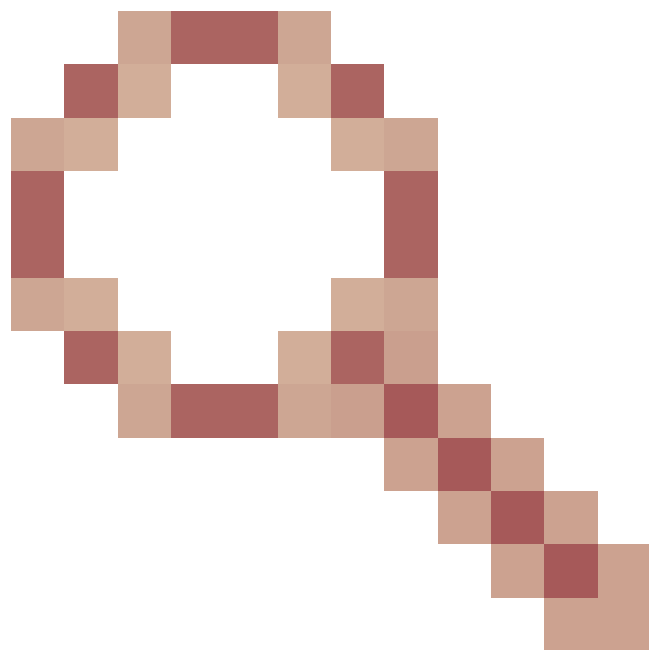
[第4步：選擇SNMP](#)

[第5步：停用SNMP伺服器](#)

[第6步：儲存到策略並進行部署](#)

[如果您已升級且發生開機回圈：](#)

簡介



本檔案介紹與Cisco錯誤ID [CSCwi63113](#)相關的資訊，以及在升級到FTD版本7.2.6期間如何防止問題。

背景

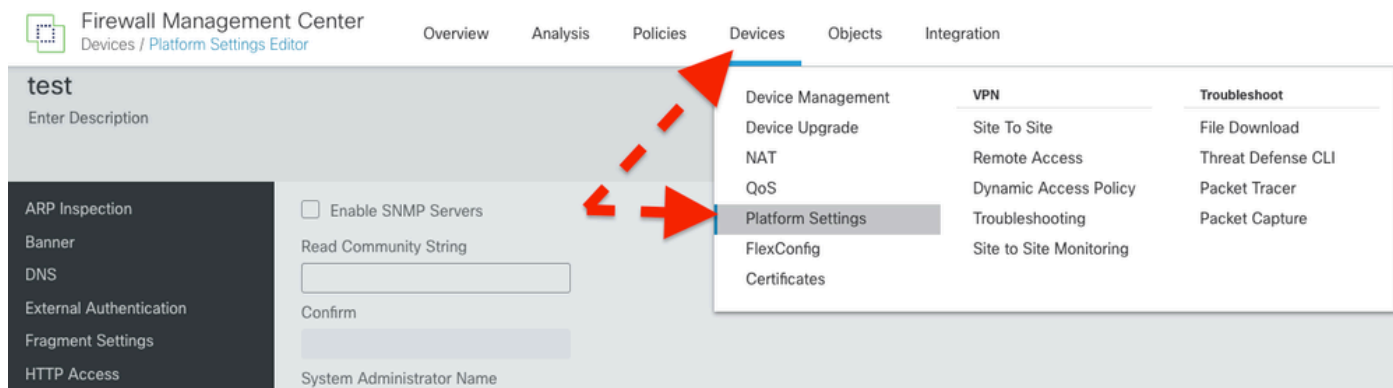
思科Firepower威脅防禦軟體版本7.2.6包含思科漏洞ID [CSCwi63113](#)，該漏洞可阻止某些裝置在啟用SNMP時啟動。在安裝7.2.6之前，請停用SNMP，直到可以升級到7.2.7或更高版本。正在對此進行修復，將於2024年5月3日發佈為7.2.7。此外，思科將在2024年5月6日前發佈7.2.5.2，即7.2.5.1，僅對CVE-2024-20353、CVE-2024-20359和CVE-2024-20358進行了修正。

升級前停用SNMP

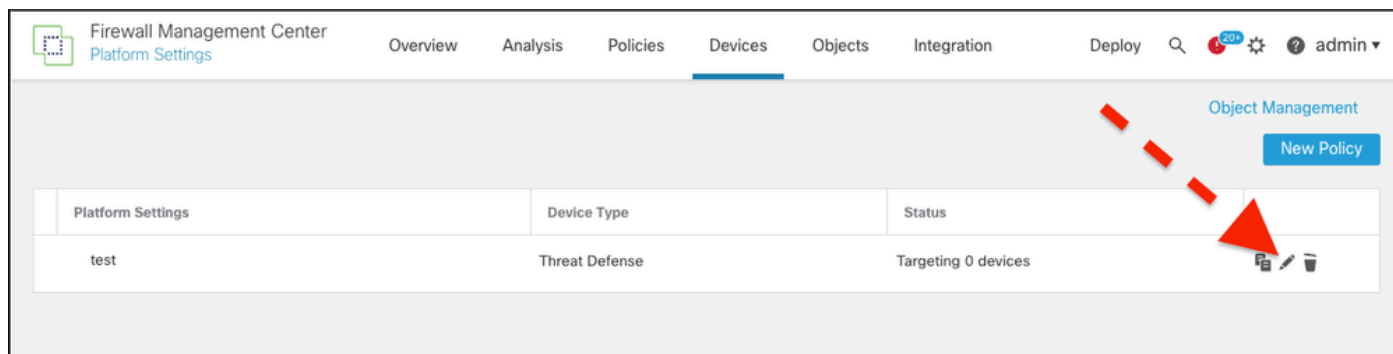
FMC步驟：

第1步：登入到FMC

第2步：導航至Devices > Platform Settings



第3步：編輯與您的FTD裝置關聯的策略



第4步：選擇SNMP



test

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port

(1 - 65535)

Hosts

Users

SNMP Traps

Interface	Network	SNMP Version	Poll/Trap
Management	backup_c1	1	Poll,Trap

第5步：停用SNMP伺服器



test

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port

(1 - 65535)

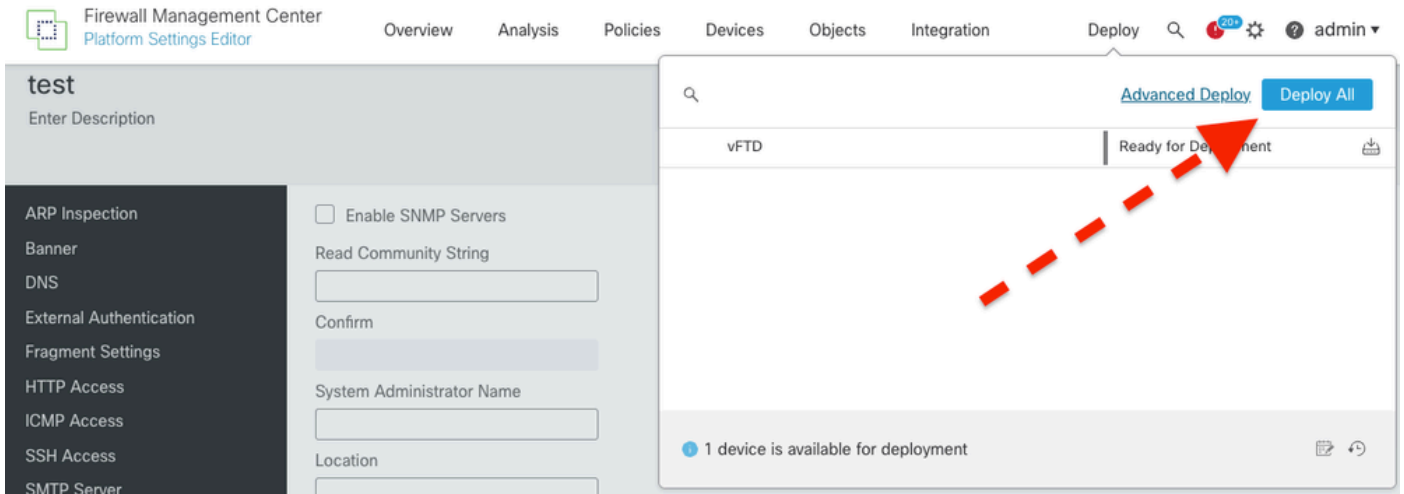
Hosts

Users

SNMP Traps

Interface	Network	SNMP Version
Management	backup_c1	1

第6步：儲存到策略並進行部署



有關詳情，請參閱此缺陷，請訪問：[思科漏洞ID CSCwi63113](#)。

如果您需要任何詳細資訊，請聯絡Cisco TAC (support.cisco.com)和參考神秘門(cisco-sa-asaftd-persist-rce-FLsNXF4h / CVE-2024-20359)

如果您已升級且發生開機回圈：

如果您已經更新到7.2.6，並且遇到思科漏洞ID [CSCwi63113](#)的影響，請與思科TAC (support.cisco.com)聯絡。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。