

Proteger contra CSCwi63113 durante a atualização para 7.2.6

Contents

[Introdução](#)

[Background](#)

[Desabilitar o SNMP antes da atualização](#)

[Etapas do FMC:](#)

[Etapa 1: Faça login no FMC](#)

[Etapa 2: Navegue até Dispositivos > Configurações da plataforma](#)

[Etapa 3: edite a política associada aos seus dispositivos de FTD](#)

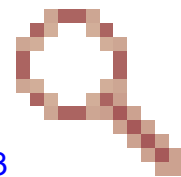
[Etapa 4: Selecionar SNMP](#)

[Etapa 5: Desative os servidores SNMP](#)

[Etapa 6: Salvar na política e implantar](#)

[O que fazer Se você já tiver atualizado e estiver passando por um loop de inicialização:](#)

Introdução



Este documento descreve informações relacionadas ao bug da Cisco ID [CSCwi63113](#) e como evitar problemas durante a atualização para o FTD versão 7.2.6.

Background

O software Cisco Firepower Threat Defense versão 7.2.6 contém o bug da Cisco ID [CSCwi63113](#), que impede que alguns dispositivos sejam inicializados quando o SNMP estiver habilitado. Antes de instalar o 7.2.6, desative o SNMP até poder atualizar para o 7.2.7 ou posterior. Uma correção para isso está sendo preparada e será lançada como 7.2.7 até 3 de maio de 2024. Além disso, a Cisco lançará a versão 7.2.5.2 até 6 de maio de 2024, que é a 7.2.5.1 com apenas as correções para CVE-2024-20353, CVE-2024-20359 e CVE-2024-20358.

Desabilitar o SNMP antes da atualização

Etapas do FMC:

Etapa 1: Faça login no FMC

Etapa 2: Navegue até Dispositivos > Configurações da plataforma

Firewall Management Center
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

test
Enter Description

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP Access

Enable SNMP Servers
Read Community String
Confirm
System Administrator Name

- Device Management
- Device Upgrade
- NAT
- QoS
- Platform Settings**
- FlexConfig
- Certificates

- VPN**
- Site To Site
- Remote Access
- Dynamic Access Policy
- Troubleshooting
- Site to Site Monitoring

- Troubleshoot**
- File Download
- Threat Defense CLI
- Packet Tracer
- Packet Capture

Etapa 3: edite a política associada aos seus dispositivos de FTD

Firewall Management Center
Platform Settings

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 20+ ⚙️ ? admin ▾

Object Management
New Policy

Platform Settings	Device Type	Status	
test	Threat Defense	Targeting 0 devices	

Etapa 4: Selecionar 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

Etapa 5: Desative os servidores 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)

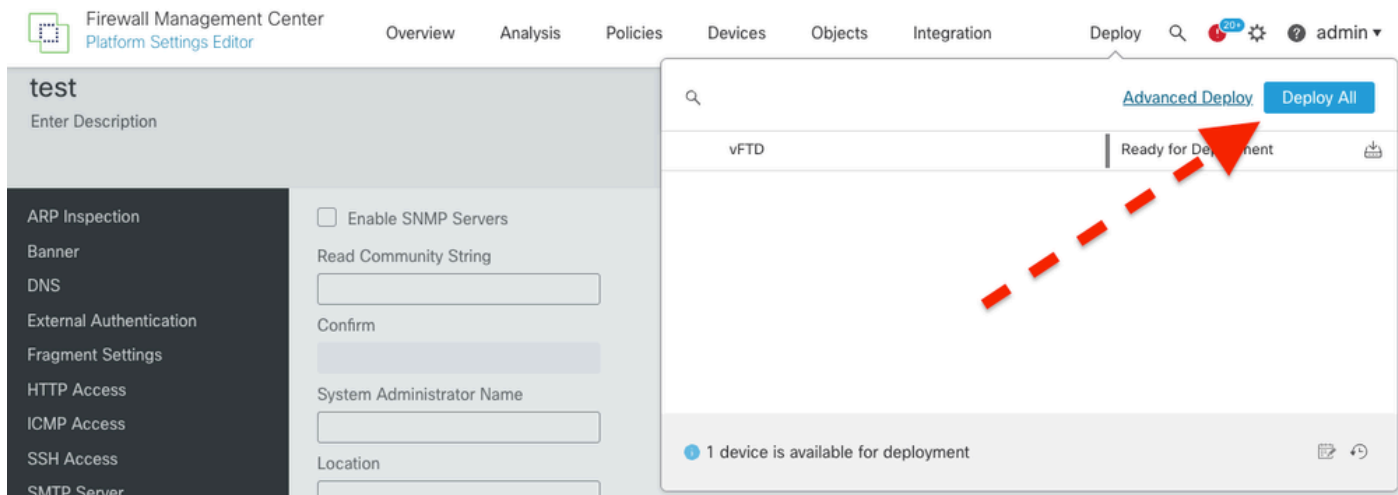
Hosts

Users

SNMP Traps

Interface	Network	SNMP Version
Management	backup_c1	1

Etapa 6: Salvar na política e implantar



Verifique o defeito para obter informações mais atualizadas: ID de bug da Cisco [CSCwi63113](https://cisco.com/ciscobug/CSCwi63113).

Se precisar de mais informações, entre em contato com o Cisco TAC (support.cisco.com) e consulte Arcane Door (cisco-sa-asaftd-persist-rce-FLsNXF4h / CVE-2024-20359)

O que fazer Se você já tiver atualizado e estiver passando por um loop de inicialização:

Se você já atualizou para a versão 7.2.6 e está enfrentando os efeitos do bug da Cisco ID [CSCwi63113](https://cisco.com/ciscobug/CSCwi63113), entre em contato com o Cisco TAC (support.cisco.com).

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.