

# Cisco DOCSIS 1.1 Vulnerability



Medium  
ID : cisco-sa-20060920-docsis

[CVE-2006-4950](#)

Published : 2006-09-20 16:00

Vulnerability ID : Final

CVSS Score : [6.0](#)

Workarounds : No Workarounds available

Cisco Reference ID : [CSCsb04965 CSCsb06658](#)

This vulnerability is a denial of service attack against the Cisco DOCSIS 1.1 protocol. It allows an attacker to send a sequence of frames to a DOCSIS 1.1 CPE (e.g., a cable modem) that causes it to drop all incoming traffic until it is reset or power-cycled.

## Description

This vulnerability is a denial of service attack against the Cisco DOCSIS 1.1 protocol.

IAD2400, IAD2400, VG224, and VG224 are Cisco Network Management Protocol (SNMP) over Cable Service Interface (OSI Layer 3) standards. They define how data is exchanged between a Cisco DOCSIS 1.1 cable modem and a Cisco router or switch. The vulnerability occurs when a malicious user sends a sequence of frames to the cable modem that causes it to drop all incoming traffic until it is reset or power-cycled.

The attack works by sending a sequence of frames to the cable modem that causes it to drop all incoming traffic until it is reset or power-cycled. This can result in significant network downtime and loss of service for users connected to the affected device.

Protocol (SNMP) over Over Cable Service Interface (OSI Layer 3) standard defines how data is exchanged between a Cisco DOCSIS 1.1 cable modem and a Cisco router or switch.

Specification (DOCSIS) version 1.1 specifies the interface between a Cisco DOCSIS 1.1 cable modem and a Cisco router or switch.

The vulnerability is triggered when a malicious user sends a sequence of frames to the cable modem that causes it to drop all incoming traffic until it is reset or power-cycled.

The attack works by sending a sequence of frames to the cable modem that causes it to drop all incoming traffic until it is reset or power-cycled. This can result in significant network downtime and loss of service for users connected to the affected device.

## Impact

This vulnerability is a denial of service attack against the Cisco DOCSIS 1.1 protocol. It allows an attacker to send a sequence of frames to a DOCSIS 1.1 CPE (e.g., a cable modem) that causes it to drop all incoming traffic until it is reset or power-cycled.

This vulnerability is a denial of service attack against the Cisco DOCSIS 1.1 protocol. It allows an attacker to send a sequence of frames to a DOCSIS 1.1 CPE (e.g., a cable modem) that causes it to drop all incoming traffic until it is reset or power-cycled.

The vulnerability is triggered when a malicious user sends a sequence of frames to the cable modem that causes it to drop all incoming traffic until it is reset or power-cycled.

```
<#root>

Router#
show snmp community

Community name: cable-docsis
Community Index: cisco0
Community SecurityName: cable-docsis
storage-type: read-only active
```

ãf‡ãf♦ã,¤ã,¹ã♦§SNMPã,µãf%ãf♦ã♦Œç„jåš¹ã♦«ã♦¤ã♦£ã♦|ã♦,,ã,<ã^ã♦^-ã€♦æ-;ã♦®ã,^ã♦

```
<#root>

Router#
show snmp community

%SNMP agent not enabled
```

Cisco

èf½å“♦ã♦§ç”¹åf♦ã♦—ã♦|ã♦,,ã,<ã,½ãf•ãf^ã,|ã,§ã,çã,’ç°èª♦ã♦™ã,<ã♦«ã♦^-ã€♦ãf‡ã♦ã,¤ã,¹ã♦version ã,³ãfžãf³ãf‰ã,’ç™°è;Œã♦—ã♦|ã,·ã,¹ãftãf ãf♦ãfŠãf¼ã,‘è;”ç¤°ã♦—ã♦¾ã♦™ã€,Cisco  
IOS å,½ãf•ãf^ã,|ã,§ã,çã♦^-ã€ŒInternet Operating System  
Softwareã♦ã♦¾ã♦ÿã♦^-ã♦~ã♦«ã♦“ã€ŒIOSã♦ã♦”è;”ç¤°ã♦•ã,Œã♦¾ã♦™ã€,å‡°åŠ›ã♦®æ-;ã♦®  
Cisco ãf‡ãf♦ã,¤ã,¹ã♦«ã♦^- show version  
ã,³ãfžãf³ãf‰ã’Œã♦¤ã,,ã♦<ã♦ç°ã♦^ã,<ã‡°åŠ›ã♦Œè;”ã♦•ã,Œã♦¾ã♦™ã€,  
æ-;ã♦®ä¾<ã♦^-ã€♦IOSãf¤ãf¤ãf¼ã,¹12.2(15)MC2ã,’å®ÿè;Œã♦—ã€♦ã,¤ãf³ã,¹ãf^ãf¼ãf¤ã♦•ã,Œã♦|ã-Mã♦§ã♦,ã,<ã,·ã,¹ã,³èf½å“♦ã,’ç¤°ã♦—ã♦|ã♦,,ã♦¾ã♦™ã€,

Cisco Internetwork Operating System Software  
IOS (tm) 1900 Software (MWR1900-I-M), Version 12.2(15)MC2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

Cisco

IOSãf¤ãf¤ãf¼ã,!ã♦®å½å♦è|♦å‰‡ã♦®è©³ç’ºã♦«ã♦¤ã♦,,ã♦|ã♦^-ã€♦<http://www.cisco.com/warp>

è,,†å½±æ€§ã♦®ã♦,ã,<èF½å“♦

è©²å½“ã♦™ã,<ã>Cisco

IOSã,½ãf•ãf^ã,|ã,§ã,çãf¤ãf¤ãf¼ã,¹ã♦§ç”¹åf♦ã♦—ã♦|ã♦,,ã,<ã,·ã,¹ã,³ãf‡ãf♦ã,¤ã,¹ã♦«ã♦^-ã€♦æ-

- Cisco IAD2430 Integrated Access Device
- Cisco IAD2431ç¶å♦^ã,çã,~ã,»ã,¹ãf‡ãf♦ã,¤ã,¹
- Cisco IAD2432 Integrated Access Device
- Cisco VG224 Analog Phone Gateway
- Cisco MWR 1900äfçãf♦ã,¤ãf«ãf~ã,¤ãf¤ãf~ã,¹ã,~ãffã,¤ãf«ãf¼ã,¿
- Cisco MWR 1941äfçãf♦ã,¤ãf«ãf~ã,¤ãf¤ãf~ã,¹ã,~ãffã,¤ãf«ãf¼ã,¿

è,,†å¼±æ€§ã,’å♦«ã,”ã♦§ã♦,,ã♦ªã♦,,ã♦”ã♦”ã♦”ã♦CEççºèªã♦•ã,CEã♦Ýè£½å”♦

è,,†å¼±æ€§ã,’å♦«ã,”ã♦§ã♦,,ã♦ªã♦,,è£½å”♦ã♦”æ¬jã♦®ã♦”ã♦Šã,Šã♦§ã♦™ã€,

- Cisco IAD2420ç¶å♦^ã,çã,~ã,»ã,¹ãf‡ãf♦ã,¤ã,¹
- Cisco IAD2421ç¶å♦^ã,çã,~ã,»ã,¹ãf‡ãf♦ã,¤ã,¹
- Cisco IAD2423ç¶å♦^ã,çã,~ã,»ã,¹ãf‡ãf♦ã,¤ã,¹
- Cisco IAD2424ç¶å♦^ã,çã,~ã,»ã,¹ãf‡ãf♦ã,¤ã,¹

ää»—ã♦®ã,·ã,¹ã,³è£½å”♦ã♦«ã♦Šã♦,,ã♦”!ã€♦ã♦”ã♦®ã,çãf‰oãf♦ã,¤ã,¶ãfãã♦®å½±éÝ,ã,’å♦—ã

è©³ç’°

## Data Over Cable Service Interface

Specification(DOCSIS)è!æ ¼ã♦®å®Ýè£...ã♦«ã,~ã,Šã€♦ã,±ãf¼ãf~ãf«ãf‡ãf~ãf—ãfãf♦ã,¤ãf€ãf¼ã  
[2669](#)ã♦§ã♦”ã€♦DOCSISæ°—æ<ã>”è!<ã>ªã♦•ã,CEã,<ã>Ýã,ã♦”ã,µãf♦ãf¼ãf~ã♦CEå¿...è!ã♦”ã

### CABLE-DEVICE-

MIBã♦”ã♦—ã♦”!ã,^ã♦”çÝ¥ã,%oã,CEã,<DOCSISã,±ãf¼ãf~ãf«ãf‡ãf♦ã,¤ã,¹MIBã♦CEå®šç¾©ã♦•ã,CE

"This table controls access to SNMP objects by network management stations. If the table is empty, access to SNMP objects is unrestricted. This table exists only on SNMPv1 or v2c agents and does not exist on SNMPv3 agents. See the conformance section for details. Specifically, for v3 agents, the appropriate MIBs and security models apply in lieu of this table."

DOCSISæ°—ã♦”æ°—æ<ã>—ã€♦SNMPã,¤ãf~ã,¤ã,§ã,~ãf~ã♦,ã♦®ç„jå^¶é™♦ã,çã,~ã,»ã,¹ã,’å»žé♦¿ã  
 docsisã€♦ã♦CEå♦”ã♦¾ã,CEã♦”!ã♦,,ã♦¾ã♦™ã€,

ã♦”ã♦®SNMPã,³ãfÝãf¥ãf~ãf~ã,¹ãf~ãf~ã,¹ã,¹ã♦”ã,♦ã,ã♦®ã,ã♦”ã€♦DOCSISæ°—æ<ã>—ã♦®ã,±ãf¼ã  
 IOSãf¤ãf¼ã,¹ãf~ãf~ã,¤ãf~ã♦§ã♦”ã♦®ã,³ãfÝãf¥ãf~ãf~ã,¹ãf~ãf~ã,¹ã,¹ã,♦ç””æ,,♦ã♦”ã,¤ãf♦ã

ã♦”ã,CEã,%oã♦®ãf—ãf©ãffãf~ãf~ã,©ãf¼ãf~ã♦§è,,†å¼±æ€§ã♦®ã♦,ã,ãf♦ãf¼ã,¤ãf§ãf~ã♦®Cisco  
 IOSã,½ãf~ãf~ã,¹ã,§ã,çã,’å®Ýè;CEã♦—ã♦”!ã♦,,ã,ã♦”ã,Šã®çæ§~ã♦”ã€♦è¿½åŠ ã♦®è”ã♦”å♦—ã,Š/æ,ã



ä, Šè~ä♦®ä¾¤ä♦§ä♦~ä€♦ä€Œno-  
 accessä€♦ä♦~ä♦„ä♦†å♦♦å%♦ä♦®æ-°ä♦—ä♦„ä,³äfÝäf¥äf<äftä,£ä♦Œä½œæ^♦ä♦•ä,Œä♦¾  
 accessä€♦ä,’ä½¿ç”“ä♦™ä,«è~±å♦~ä♦~ä€♦ä,çä,~ä,»ä,¹äfªä,¹äf^ä♦«ä,^ä♦£ä♦|å^¶å¾jä♦•ä,Œä♦¾  
**mib community-map**,³äfžäf³äf%oä♦®è½åŠ ä♦«ä,^ä,Šä€♦ä€Œcable-  
 docsisä€♦ä♦®ç♦¾åœ~ä♦®ä,³äfÝäf¥äf<äftä,£ä,¹äf^äfªä,ºä~ä€♦æ-°ä♦—ä♦„ä,³äfÝäf¥äf<äft  
 accessä€♦ä♦®ä,çä,~ä,»ä,¹å^¶é™♦ä♦®ä,«ä♦«ç½®ä♦«ä,Œä€♦ä€Œcable-  
 docsisä€♦ä,³äfÝäf¥äf<äftä,£ä,¹äf^äfªä,ºä~ä½¿ç”“ä♦§ä♦~ä♦~ä♦~ä,Šä♦¾ä♦™ä€,  
 ä,³äf³äf^äf½äf«äf—äf~äf½äf³äf♦äfªä,·äf³ä,°

Cisco

IOSäfªäfªäf½äf,¹äf^äf~ä,¤äf³12.0Sä♦12.2SXä♦12.2Sä♦12.3Tä♦12.4ä€♦ä♦Šä,^ä♦¾12.4Tä♦~ä€♦

```

access-list 111 deny udp host 10.1.1.1 host 192.168.10.1 eq snmp
access-list 111 permit udp any any eq snmp
access-list 111 deny ip any any
!
class-map match-all drop-snmp-class
  match access-group 111
!
!
policy-map drop-snmp-policy
  class drop-snmp-class
    drop
!
control-plane
service-policy input drop-snmp-policy
  
```

12.0Sä♦12.2Sä♦ä♦Šä,^ä♦¾12.2SXä♦®Cisco

IOSäf^äf~ä,¤äf³ä♦§ä♦~ä€♦äf♦äfªä,·äf½äfžäffäf—ä♦®æñ<æ-‡ä♦Œç•°ä♦~ä,«ä♦~ä♦~ä♦~ä♦~æ³..æ,,

```

policy-map drop-snmp-policy
  class drop-snmp-class
    police 32000 1500 1500 conform-action drop exceed-action drop
  
```

ä,Šè~ä♦®CoPPä♦®ä¾¤ä♦§ä♦~ä€♦ä€Œpermitä♦ä,çä,~ä,·äf§äf³ä,‘æŒ♦ä♦¤ä,~ä,~ä,¹äf—äfä,¤äf

CoPP æ©Ýèf½ä♦®è~å®šä♦~ä½¿ç”~æ-¹æ³•ä♦~ä♦¤ä,“ä♦¤ä|ä♦®è©³ç’°ä♦~ä€♦æ-¡ä♦®  
 URL ä♦§çç°è~ä♦§ä♦~ä♦~ä♦¾ä♦™ä€,

[http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t4/feature/gtrtlmt.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/gtrtlmt.html)

æ½é½ã»šã»ã, <ãf>ã, **1ãf^ã** **ã'ã»ã,çã,-ã,»ã, 1ã,'å^¶é™** **ã™ã,** <

ã,çã,-ã,»ã, **1ã, 3ãf³ãf^ãf** **1/4ãf** «ãf<sup>a</sup>ã, **1ãf^**(ACL)ã, **'ã½ç"** **ã—ã** | **ã€#ãffãf** **ã,¤ã, 1ã#ã®ãf^ãf** ©ãf•ã, **Eãffã**  
IOSãf#ãf **ã,¤ã, 1ã#ã»ã** **—ã** **ã#ã**, **3ãf** **Ýãf** **ãf&ftã, Eã,** **1ãf^ãf** **ãf³ã, °ã** **”ã#ã»SNMPè** **| #æ±,ã#ã®é#ã**  
docsisã, **3ãf** **Ýãf** **ãf&ftã, Eã,** **1ãf^ãf** **ãf³ã, °ã** **”è”ã®šã,ãf—ã,** ·ãfSãf³ã, **'ã½ç"** **ã—ã** | **ã¤%** **æ»’ã** **3/4ã#ã** **å**

ã,¤ãf³ã, **çãf** **1/4ãf** •ã, **§ã,¤ã, 1ACL**ã, **'ã½ç"** **ã—ã** | **ã€#æ½é½ã, IPã,çãf%** **øãf—ã, 1ã#ã<ã, %oãf»ãf** **1/ã,**

**æ”í/šSNMP**ã **—UDP**ã **«ã** **Ý** **øã#,,ã#ã** | **ã#,,ã,ã#Ýã, ?ã€#é#ãæ½jå...fã** **®IPã,çãf%** **øãf—ã, 1ã,’ã, 1ãf-**

æ—ã **®æ½jå½µã,çã,-ã,»ã, 1ãf<sup>a</sup>ã, 1ãf^ã, ‘ãf#ãffãf^ãf** **ãf** **1/4ã, —ã** **»ã»é#©ç"** **ã#** **ã#ã#ã#ã#3/4ã#™ã** **é#æ—jã#**  
IP **ã,çãf%** **øãf—ã, 1** **192.168.10.1** **ã#** **Šã, ^ã#** **3** **172.16.1.1**

ã#Œè”ã®šã#•ã,Œã# | **ã#,,ã,ã#”ã# “ã€#ã#™ã** **1ã# | ã#®SNMP** **ã,çã,-ã,»ã, 1ã#ŒIP**  
**ã,çãf%** **øãf—ã, 1** **10.1.1.1**

ã#®ç®jç#tã, **1ãf&ftã** **1/4ã, ·ãfSãf³ã** **«é#** **ã®šã#•ã,Œã# | ã#,,ã,ã#”ã# “ã€#ã#Šã, ^ã#** **3ã#?** **ã#®ç®c**

IP

ã,çãf%**øãf—ã, 192.168.10.1** **ã# “ã#** **ã#’é#šãæ½jã#™ã**, **<ã¿...è| #ã#Œã#ã,ã,ã#”ã# “ã#** **ã#** **çãf** **™ã** **é#,**

access-list 101 permit udp host 10.1.1.1 host 192.168.10.1 eq snmp

access-list 101 deny udp any host 192.168.10.1 eq snmp

access-list 101 deny udp any host 172.16.1.1 eq snmp

access-list 101 permit ip any any

ã#æ½ã#®å¾Œã#æ½é#æ½®è”ã®šã, **3ãfžãf³ãf%** **øã, 'ã½ç"** **ã—ã** | **ã€#ã#™ã** **1ã# | ã#®ã,¤ãf³ã,çãf³ã,**

interface FastEthernet 0/0

ip access-group 101 in

ãf»ãf

IP

ã,çãf%**øãf—ã, 1ã#Œå¤šæ•°è”ã®šã#•ã,Œã# | ã#,,ã,ãf&ftã** **ã,¤ã, 1ã#** **ã#3/4ã#Ýã#—ãf** **ãf** **1/4ã, çã#”é#šãæ½jã#™ã**

ã,¤ãf³ãf•ãf©ã, **1ãf^ãf** ©ã, **—ãf#ãf&ft**E ACL**ï½^i**ACL**ï½^o**

ãf#ãffãf^ãf

ACL **ã#—ãf#ãffãf^ãf** **ãf** **1/4ã, —ã, »ã,ãf¥ãf** **ã&ftã, Eã#®ãf™ã, 1ãf**

ãf—ãf©ã, **—ãf&ftã, Eã, 1ã#** **”è#fã#^ã, %oã,Œã# | ã#** **Šã, Sã#** **ã#”ã#** **”ã#** **”ã#** **Šã#®ç%** **1** **ã®šã#®è,,** **tå½æ#ëã**



è©²å½“ã¢™ã, < 12.3 ãƒ™ãƒ¼ã,¹ã¢®ãƒãƒªãƒ¼ã,¹	ãƒªãƒ“ãƒ«ãƒ‰	ãƒ;ãƒ³ãƒ†ãƒŠãƒ³ã,¹
	12.3(4)T13	
	12.3(7)T11	
12.3T	12.3(8)T10	
	12.3(11)T6	
	è,,†å¼±æ€§ï¼š12.3(14)ã¢Šã¢—12.4(1b)ä»¥é™♦ã¢«ç§»è;Œ	
12.3XD	è,,†å¼±æ€§ã¢,ã,Šã€♦12.3(7)T11ä»¥é™♦ã¢«ç§»è;Œ	
12.3XX	è,,†å¼±æ€§ã¢,ã,Šã€♦12.4(1b)ä»¥é™♦ã¢«ç§»è;Œ	
12.3XY	è,,†å¼±æ€§ã¢,ã,Šã€♦12.4(1b)ä»¥é™♦ã¢«ç§»è;Œ	
12.3YA	è,,†å¼±æ€§ã¢,ã,Šã€,TACã¢«ã¢Šå•♦ã¢„å¢^ã,♦ã¢>ã¢♦ã¢ã¢ã¢ã¢	
12.3YD	è,,†å¼±æ€§ã¢,ã,Šã€♦12.4(2)T5ä»¥é™♦ã¢«ç§»è;Œ	
12.3YF	è,,†å¼±æ€§ã¢,ã,Šã€♦12.3(14)YXä»¥é™♦ã¢«ç§»è;Œ	
12.3YG	12.3(14)YG5	
12.3YH	è,,†å¼±æ€§ã¢,ã,Šã€♦12.4(2)T5ä»¥é™♦ã¢«ç§»è;Œ	
12.3YI	è,,†å¼±æ€§ã¢,ã,Šã€♦12.4(2)T5ä»¥é™♦ã¢«ç§»è;Œ	

12.3YJ	è,,†å¼±æ€§ã,ã,Šã€♦12.3(14)YQ8ä»¥é™♦ã♦«ç§»è;Œ	
12.3YK	è,,†å¼±æ€§ã,ã,Šã€♦12.4(4)Tä»¥é™♦ã♦«ç§»è;Œ	
12.3YM	12.3(14)YM8	
12.3YQ	12.3(14)YQ8	
12.3YS	è,,†å¼±æ€§ã,ã,Šã€♦12.4(4)Tä»¥é™♦ã♦«ç§»è;Œ	
12.3YT	è,,†å¼±æ€§ã,ã,Šã€♦12.4(4)Tä»¥é™♦ã♦«ç§»è;Œ	
12.3YU	è,,†å¼±æ€§ã,ã,Šã€♦12.4(2)XBä»¥é™♦ã♦«ç§»è;Œ	
è©²å½“ã♦™ã, ãf™ãf¼ã,¹ã♦®ãfãfãf¼ã,¹	ãfãf“ãf<ãf% ãf;ãf³ãf†ãfŠãf³ã,¹	
12.4	12.4(1b)	12.4(3)
12.4MR		12.4(4)MR
12.4T	12.4(2)T5	12.4(4)T

ä,♦æ£å^©ç”“äº<ä¾<ã♦”“å...¬å¼♦ç™oè;“

Cisco PSIRT

ã♦Šã“ã€♦æœ¬ã,çãf%oãf♦ã,¤ã,¶ãfã♦«è”“è¼‰oã♦•ã,Œã♦!ã♦,,ã,<è,,†å¼±æ€§ã♦®ã,♦æ£å^©ç”“

ã♦”ã♦®è,,†å¼±æ€§ã“ã€♦ã♦Šã®çæ§~ã♦<ã,%oã,·ã,¹ã,³ã♦“å ±å’Šã♦•ã,Œã♦Ýã,,ã♦®ã♦§ã♦™ã€,

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060920-docsis>

## æ”’è”,å±¥æ’

ãf <sup>a</sup> ãf“ã, ,ãf§ãf <sup>3</sup> 1.0	2006å¹’9æœ^20æ—¥	å^♦å›žå...¬é-<ãf <sup>a</sup> ãf <sup>a</sup> f¼ã, <sup>1</sup>
--	------------------	---

## å^©ç”’è!♦ç’,,

æœ¬ã, çãf%oãf♦ã,¤ã, ¶ãf<sup>a</sup>ã♦ç„jäç♦è”¼ã♦®ã,,ã♦®ã♦”ã♦—ã♦|ã♦”æ♦♦ä¾ã♦—ã♦|ã♦Šã,Šã€æœ¬ã, Çãf%oãf♦ã,¤ã, ¶ãf<sup>a</sup>ã♦®æf...å ±ã♦Šã, ^ã♦³ãf<sup>a</sup>ãf<sup>3</sup>ã, —ã♦®ä½¿ç””ã♦«é-çã♦™ã, <è²¬ã»»ã♦®ã, €ã♦¾ã♦Ýã€♦ã,·ã,¹ã,³ã♦—æœ¬ãf%oã,ãf¥ãf;ãf<sup>3</sup>ãf^ã♦®å†...å®¹ã,’ä°^å’Šã♦^ã♦—ã♦«å¤%oæ»ã♦—ã♦æœ¬ã, çãf%oãf♦ã,¤ã, ¶ãf<sup>a</sup>ã♦®è”~è\_°å†...å®¹ã♦«é-çã♦—ã♦|æf...å ±é...♦äç;ã♦® URL  
ã,’çœ♦ç•¥ã♦—ã€♦å♦~ç¬ã♦®è»çè¼%oã,,æ,,♦è”³ã,’æ-½ã♦—ã♦Ýå ’å♦^ã€♦å½”ç¤¾ã♦Œç®;ç♦ã♦”ã♦®ãf%oã,ãf¥ãf;ãf<sup>3</sup>ãf^ã♦®æf...å ±ã♦—ã€♦ã,·ã,¹ã,³è£½å”♦ã♦®ã, ”ãf<sup>3</sup>ãf%oãf|ãf¼ã, ¶ã,’å”¾è±;ã

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。