Cisco IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®Session Initiation Protocolã€«ã€Šã€'ã,‹Denial of Service(DoS)ã€®è„†å¼±æ€§

High

ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƪãƼID : cisco-sa-20131106-sip

åˆ€å…¬é–‹æ—¥ : 2013-11-06 16:00

æœ€çµ‚æ›´æ–°æ—¥ : 2013-11-15 16:42

ãƒ€ãƼãƸãƧãƳ 1.1 : Final

CVSSã,¹ã,³ã,¢ : 7.8

å›žé¿ç– : No Workarounds available

Cisco ãƒ€ã,° ID : CSCuc42558

CVE-2013-5553

æ—¥æœ¬èªžã€«ã,ˆã,‹æƒ…å ±ã€¯ã€€è‹±èªžã€«ã,ˆã,‹åŽŸæ–‡ã€®é€žå…¬å¼€ã

æ¦‚è¦

Cisco IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®Session Initiation Protocolï¼ˆSIPï¼‰ã,»ãƒƒã,·ãƧãƳé–‹å§‹ãƒ—ãƒˆã,³ãƫï¼‰å®Ÿè£…ã€«ã€¯è„†å¼±æ€§ã€Œå˜œ¨ã€—ã€¾ã€™ã€,èª€è¨¼ã€•ã,Œã€¦ã€„ã€IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƪãƪãƼã,¹ã€Œå½±éŸ¿ã,'å€—ã€'ã€¾ã€™ã€,

ã,·ã,¹ã,³ã€¯ã€"ã€®è„†å¼±æ€§ã€«å¯¾å‡¦ã€™ã,‹ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒƒãƒ—ãƒ‡ãƼãƒˆã,'ãƪãƪãƼ

SIPã,'å®Ÿè¡Œã€™ã,‹å¿…è¦ã€Œã€,ã,‹ãƒ‡ãƒ€ã,¤ã,¹ã€«å¯¾ã€™ã,‹å›žé¿ç–ã€¯ã€,ã,Šã€¾ã€›ã

ã€"ã€®ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƪã€¯ã€€æ¬¡ã€®ãƪãƳã,¯ã,ˆã,Šç¢ºèª€ã€§ã€€ã€¾ã€™ã€,
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131106-sip

è©²å½"è£½å"

è„†å¼±æ€§ã€®ã€,ã,‹è£½å"

ã,·ã,¹ã,³ãƒ‡ãƒ€ã,¤ã,¹ã€¯ã€SIPãƒ¡ãƒƒã,»ãƼã,¸ã,'å‡¦ç†ã€™ã,‹ã,ˆã†ã€«è¨å®šã€•ã,Œã€Ÿè©²
IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƪãƪãƼã,¹ã,'å®Ÿè¡Œã€—ã€¦ã€„ã,‹å ´å€ˆã€«å½±éŸ¿ã,'å€—ã€'ã€¾ã€
IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƪãƪãƼã,¹ã€Œã€"ã€®è„†å¼±æ€§ã€®å½±éŸ¿ã,'å€—ã€'ã€¾ã€™ã€,

- 15.1(4)GCã€Šã‚ˆã€³15.1(4)GC1
- 15.1(4)M4ã€œ15.1(4)M5ã€œã€Šã‚ˆã€³15.1(4)M6

Cisco
IOSã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã€®æœ€è¿‘ã€®ãƒªãƒªãƒ¼ã‚¹ã€¯ã€œãƒ‡ãƒ•ã‚©ãƒ«ãƒˆã§SIPãƒ¡ãƒƒ
dial-peer
voiceè¨å®šã‚„ãƒžãƒƒãƒ‰ã‚™ç™ºè¡Œã€—ã€¦ãƒ€ã‚¤ãƒ¤ãƒ«ãƒ”ã‚¢ã‚’使ç”™ã€™ã‚‹ã€¨ã€SIPãƒ—ã‚
IOSãƒ‡ãƒ•ã‚©ãƒ«ãƒˆã§SIPãƒ¡ãƒƒã‚»ãƒ¼ã‚¸ã€Œå‡¦ç††ã•ã‚Œã€™ã€ã¾ãŸã€ePhoneã€
Unified Communications Manager
Expressã€®ä¸€éƒ¨ã€®æ©Ÿèƒ½ã‚„ã€œè¨å®šã•ã‚Œã‚‹ã¨ SIPãƒ—ãƒã‚»ã‚¹ã‚’èˆªå‹•çš„ã«é–‹å§‹

```
!
 dial-peer voice <Voice dial-peer tag> voip
 ...
!
```

Cisco
IOSãƒ‡ãƒ•ã‚©ãƒ«ãƒˆã®è¨å®šã‚’è¤¿ã€¹ã€¦ã€ãƒ‡ãƒ•ã‚©ãƒ«ãƒˆã«SIPãƒ¡ãƒƒã‚»ãƒ¼ã‚¸ã‚’å‡¦ç†ã€•ã€
dial-peerã€³ãƒžãƒ³ãƒ‰ã‚’ç¢ºèª€ã€™ã‚‹ã€ ã€‘ã€§ã€ªã€€ã€€ã€€ç®¡ç††è€…ã€¯ **show processes | include SIP**ã€³ãƒžãƒ³ãƒ‰ã‚’使ç”¨ã€—ã€¦ã€€Cisco
IOSã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã€®SIPãƒ¡ãƒƒã‚»ãƒ¼ã‚¸ã‚’å‡¦ç†ã€™ã‚‹ãƒ—ãƒã‚»ã‚¹ã‚’å®Ÿè¡Œã€—ã€¦ã€
IOSãƒ‡ãƒ•ã‚©ãƒ«ãƒˆSIPãƒ¡ãƒƒã‚»ãƒ¼ã‚¸ã‚’å‡¦ç†ã—ã€¾ã€™ã€‚

```
Router# show processes | include SIP
 149 Mwe 40F48254            4          1    400023108/24000  0 CCSIP_UDP_SOCKET
 150 Mwe 40F48034            4          1    400023388/24000  0 CCSIP_TCP_SOCKET
```

æ³¨ï¼šš Cisco
**IOSã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã®å®Ÿè¡Œã—ã€—ã€¦ã„ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã€ã€ã€

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€Œç¨¼åƒ�ã€—ã€¦ã€„ã,‹ã€“ã€¨ã,’ç¢ºèª�ã€§ã€��ã€¾ã€™ã€‚
ã€��ã€®å¾Œã,€ã€«ã,¤ãƒ¡ãƒ¼ã,¸å€¤ã€Œæ‹¬å¼§ã€®é–“ã€«è¡¨ç¤ºã€•ã,Œã€€ç¶šã€„ã€¦
"Version" ã€¨ Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,¨ã,¢
ãƒªãƒªãƒ¼ã,¹å€¤ã€Œè¡¨ç¤ºã€•ã,Œã€¾ã€™ã€‚ä»–ã€®ã,·ã,¹ã,³
ãƒ‡ãƒ€ã,¤ã,¹ã€§ã€¯ã€**show version**
ã,³ãƒžãƒ³ãƒ‰ã€Œå˜åœ¨ã€—ã€ªã€‹ã€£ã€Ÿã,Šã€€å^¥ã€®å‡ºåŠ›ã€Œè¡¨ç¤ºã€•ã,Œã€Ÿã

æ¬¡ã€®ä¾‹ã€¯ã€€Cisco
IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹15.0(1)M1ã,’å®Ÿè¡Œã€—ã€€ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ã€•ã,Œã€¦ã€
UNIVERSALK9-Mã€§ã€,ã,‹ã,·ã,¹ã,³è£½å“€ã,’ç¤ºã€—ã€¦ã€„ã€¾ã€™ã€‚

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

!â€“- output truncated
```

Cisco
IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã€®å‘½å��è¦�å‰‡ã€®è¿½åŠ æƒ…å ±ã€¯ã€€ãƒ›ãƒ¯ã,¤ãƒˆãƒš
IOS and NX-OS Software Reference Guideã€€(
http://www.cisco.com/web/about/security/intelligence/ios-ref.html)ã,’å€,ç…§ã€—ã€¦ã€€ã€•ã€„ã€€,

è„†å¼±æ€§ã,’å«ã,“ã€§ã€„ã€ªã€„ã€“ã€¨ã€Œç¢ºèª�ã€•ã,Œã€Ÿè£½å“€

Cisco IOS XEã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€Šã,^ã€³Cisco Unified Communications
Managerã€¯ã€€ã€“ã€®è„†å¼±æ€§ã€®å½±éŸ¿ã,’å—ã‘ã€¾ã€›ã,“ã€‚ä»–ã€®ã,·ã,¹ã,³è£½

è©³ç´°

SIPã€¯ã€€ã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã‚§ãƒ¼ã,¹ã€©ã€®IPãƒ•ã‚§ãƒ¼ãƒ¼ã,¯ã,’ä»‹ã—ã€—ã€ŸéŸ³å£°ã€Šã,^ã
Layer
Security(TLS)ã,’ã€€åŸºç›¤ã€¨ã€ªã,‹ãƒˆãƒ©ãƒ³ã,¹ãƒ•ãƒ¼ãƒˆãƒ—ãƒãƒˆã,³ãƒ«ã€¨ã€—ã€¦ä½¿ç”¨ã€

Cisco IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®Session Initiation
Protocol(SIP)æ©Ÿèƒ½ã€®è„†å¼±æ€§ã€«ã,^ã,Šã€€è²ªè¨¼ã€•ã,Œã€¦ã€„ã€ªã€„ãƒªãƒ¼ãƒˆã

ã�“ã�®è„†å¼±æ€§ã�¯ã€�ç‰¹å^¥ã�«å·§å¦™ã�«ç´°å·¥ã�•ã,Œã�ŸSIPãƒ¡ãƒƒã,»ãƒ¼ã,¸ã�®ä¸€é

ã�“ã�®è„†å¼±æ€§ã�¯ã€�Cisco IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,’å®Ÿè¡Œã�—ã�¦ã�„ã,‹ãƒ‡ãƒ�ã,¤ã,¹ã�Œã€�ç‰¹å®šã�®æœ‰åŠ¹ã�ªSI over IPv4ã�¾ã�Ÿã�¯IPv6é€šä¿¡ãƒ—ãƒãƒˆã,³ãƒ«ã�§ä¸€æ£å^©ç”¨ã�•ã,Œã,‹å�¯èƒ½æ€§ã�Œã�,ã,Šã

æ³¨ï¼šSIPã�ŒTCPãƒˆãƒ©ãƒ³ã,¹ãƒ�ãƒ¼ãƒˆä¸Šã�§å®Ÿè¡Œã�•ã,Œã�¦ã�„ã,‹å ´å�^ã�¯ã€�ã�“ã®

ã�“ã�®è„†å¼±æ€§ã�¯ã€�Cisco Bug ID CSCuc42558(ç™»éŒ²ãƒ¦ãƒ¼ã,¶å°,ç”¨)ã�Šã,^ã�³ CSCug25383(ç™»éŒ²ãƒ¦ãƒ¼ã,¶å°,ç”¨)ã�¨ã�—ã�¦æ–‡æ›¸åŒ–ã•ã,Œã�¦ã�„ã¾ã™ã€,ã“ã®è„†å¼±æ€§ã
Vulnerabilities and Exposures(CVE)IDã�¨ã�—ã�¦CVE-2013-5553ã�Œå‰²ã,Šå½“ã�¦ã,‰ã,Œã�¦ã�„ã¾ã™ã€,

å›žé�¿ç–

è©²å½“ã�™ã,‹Cisco IOSãƒ‡ãƒ�ã,¤ã,¹ã�§VoIPã,µãƒ¼ãƒ“ã,¹ç”¨ã�®SIPã�Œå¿…è¦�ã�ªå ´å�^ã€�SIPã,’ç„¡åŠ¹ã�«ã�™ã,

ãƒ�ãƒƒãƒˆãƒ¯ãƒ¼ã,¯å†…ã�®Ciscoãƒ‡ãƒ�ã,¤ã,¹ã�«é©ç”¨å�¯èƒ½ã�ªä»–ã�®ç·©å’Œç–«ã�«ã�¤ã and Mitigating Exploitation of the Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilityã€�ã,’å�,ç…§ã�—ã�¦ã��ã• ã�•ã�„ã€, https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=31516

SIPãƒªã,¹ãƒ‹ãƒ³ã,°ãƒ�ãƒ¼ãƒˆã�®ç„¡åŠ¹åŒ–

SIPã,’æœ‰åŠ¹ã�«ã�™ã,‹å¿…è¦�ã�Œã�ªã�„ã,¤ã,¹ã�®å ´å�^ã€�æœ€ã,,ç°¡å�˜ã�§åŠ¹æ IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ä¸€éƒ¨ã�®ãƒªãƒªãƒ¼ã,¹ã�§ã�¯ã€�ç®¡ç�†è€…ã�¯æ¬¡ã�®ã,³ãƒžãƒ³ãƒ‰

```
sip-ua
 no transport udp
 no transport tcp
 no transport tcp tls
```

è¦å‘Šï¼š Media Gateway Control Protocol(MGCP)ã�¾ã�Ÿã�¯H.323ã,³ãƒ¼ãƒ«ã,’å‡¦ç�†ã�—ã�¦ã„ã,‹ãƒ‡ãƒ�ã,¤ã,¹ã�«ã�“ã�®å›ž

ã€“ã€®å›žé¿ç–ã€®é€©ç”¨ä¾Œã€«ã€€ **show udp connections**ã€€ **show tcp brief all**ã€€ã€Šã‚ã€³ **show control-plane host open-ports**ã‚³ãƒžãƒ³ãƒ‰ã‚’使用ã€—ã€¦ã€€SIP UDPãƒ•ãƒ¼ãƒˆã€¨TCPãƒ•ãƒ¼ãƒˆã€Œé–‰ã€˜ã€¦ã€„ã‚‹ã€“ã€¨ã‚’確èª€ã€§ã€€ã€¾ã€™ã€

使ç”¨ã€—ã€¦ã€„ã‚‹Cisco IOSã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ã€¹ã€«ã‚ˆã€£ã€¦ã€¯ã€€SIPã€Œãƒ‡ãƒ£ãƒ«ã‚»ãƒ¼ãƒ–ãƒ«ã€«ã€ªã€£ã€£ã **show ip sockets**ã‚³ãƒžãƒ³ãƒ‰ã€®å‡ºåŠ›ã€«SIPãƒ•ãƒ¼ãƒˆã€Œé–‹ã€„ã€¦ã€„ã‚‹ã€“ã€¨ã€Œå¼•ã€€ç¶šã

```
*Nov 2 11:36:47.691: sip_udp_sock_process_read: SIP UDP Listener is DISABLED
```

ã‚³ãƒˆãƒãƒ« ãƒ—ãƒ¬ãƒ¼ãƒ³ ãƒ•ã‚ªã‚·ã‚°

SIPã‚µãƒ¼ãƒ“ã‚¹ã‚’æ€¾ä¾›ã€™ã‚‹å¿…è¦ã€Œã€,ã‚‹ãƒ‡ãƒã‚¤ã‚¹ã€¹ã€§ã€¯ã€€ã‚³ãƒˆãƒãƒ«ãƒ—ãƒ¬ãƒ¼ãƒ³ IOSã‚ªãƒªãƒ¼ã‚¹ã€¹12.0Sã€€12.2SXã€€12.2Sã€€12.3Tã€€12.4ã€€ã€Šã‚ˆã€³12.4Tã€§ã‚µãƒ€ãƒ¼ãƒ CoPP ã‚’è¨å®šã€—ã€¦ã€€ç®¡ç€†ãƒ—ãƒ¬ãƒ¼ãƒ³ã€¨ã‚³ãƒˆãƒãƒ« ãƒ—ãƒ¬ãƒ¼ãƒ³ã‚’ä¿è·ã€—ã€€æ—¢å˜ã€®ã‚»ã‚¥ãƒªãƒ†ã‚£ ãƒ¡ã‚«ãƒ‹ã‚ºãƒ ã€Šã‚ˆã€³è¨å®šã€«å¾“ã€£ã€¦ã€€ã€¤ãƒ³ãƒ•ãƒ©ã‚¹ãƒˆãƒ©ã‚¯ãƒãƒ£ ãƒ‡ãƒã‚¤ã‚¹ã€¸ã€®ãƒˆãƒ©ãƒ•ã‚£ãƒ

```
!â€“ The 192.168.1.0/24 network and the 172.16.1.1 host are trusted.
!â€“ Everything else is not trusted. The following access list is used
!â€“ to determine what traffic needs to be dropped by a control plane
!â€“ policy (the CoPP feature): if the access list matches (permit)
!â€“ then traffic will be dropped and if the access list does not
!â€“ match (deny) then traffic will be processed by the router.

access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061
access-list 100 deny udp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5060
access-list 100 deny tcp host 172.16.1.1 any eq 5061
access-list 100 permit udp any any eq 5060
access-list 100 permit tcp any any eq 5060
access-list 100 permit tcp any any eq 5061

!â€“ Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!â€“ traffic in accordance with existing security policies and
!â€“ configurations for traffic that is authorized to be sent
!â€“ to infrastructure devices.
!â€“ Create a Class-Map for traffic to be policed by
!â€“ the CoPP feature.
```

```
class-map match-all drop-sip-class
  match access-group 100

!â€“ Create a Policy-Map that will be applied to the
!â€“ Control-Plane of the device.

policy-map control-plane-policy
 class drop-sip-class
  drop

!â€“ Apply the Policy-Map to the Control-Plane of the
!â€“ device.

control-plane
 service-policy input control-plane-policy
```

æ³¨ï¼šSIPã¯ãƒˆãƒ©ãƒ³ã‚¹ãƒãƒ¼ãƒˆãƒ—ãƒãƒˆã‚³ãƒ«ã¨ã—ã¦UDPã‚’使用ã—ã¦ã„ã‚‹ã€‚
http://www.cisco.com/web/about/security/intelligence/unicast-rpf.htmlã‚’å‚ç…§ã—ã¦ãã ã•ã„ã€‚

ä¸Šè¨˜ã®CoPPã®ä¾‹ã§ã¯ã€ª"¨ã®å¯¾è±¡ã¨ã—ã¦ã€ãƒ‘ã‚±ãƒƒãƒˆã¨ã€Œpermitæ©Ÿèƒ½ã®è¨®šã¨ä½¿ç”¨ã«é–¢ä™ã‚‹è©³ç´°ã¯ã€
http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html ãŠã‚ˆã³
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html
ã‚’å‚ç…§ã—ã¦ãã ã•ã„ã€‚

ä¿®æ£æ¸ˆã¿ã½ãƒ•ãƒˆã¦ã§ã¢

ã½ãƒ•ãƒˆã¦ã§ã®ã¢ãƒƒãƒ—ã°ãƒ¼ã‚¸ãƒ§ãƒ³ã'æ¤œè¨Žã™ã‚‹å ´å^ã¯ã€
http://www.cisco.com/go/psirt ã®ã‚ˆã†ã‚³ ã‚»ã‚ƒãƒ¥ã‚¥ãƒªãƒ†ã‚£
ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªãƒ¼ã€œæ”€ã€‚ã‚Šã‚ˆã³é€šçŸ¥ã®ã¢ã‚¢ã‚«ã‚¦ãƒ³ãƒˆã€œå¾Œç¶šã®ã¢ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªãƒ¼ã€‚ãƒ‰ã‚ˆã³ã‚¢ãƒ©ãƒ¼ãƒˆã‚’å¼°è³‡ã—ã¦ãã ã•ã„ã€‚

ã„ã‚Œã‚‚Technical Assistance Centerï¼ˆTACï¼‰ã‚ã—ã€ã¾ãŸã¯ã¢ã„ã‚ãƒ¡ãƒ³ãƒˆãƒŠãƒ³ã‚¹ãƒ—ãƒãƒã‚¤ãƒ€ã«ã«

Cisco IOS ã½ãƒ•ãƒˆã¦ã§ã¢

æ¬¡ã®Cisco IOSã½ãƒ•ãƒˆã¦ã§ã¢ãƒªãƒªãƒ¼ã‚¹ã«ã¯ã€Cisco IOSã½ãƒ•ãƒˆã¦ã§ã¢ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã¹ãƒªãƒªãƒ¼ã‚¹ã«ã¯ã€ç‰¹å®šã®ãƒãƒ¬ã‚¤ãƒ³ã‚¢ãƒƒãƒ—ã«ã€Fixed Release]åˆ—ã«è¡¨ç¤ºã•ã,Œã¾ã™ã€‚ã‚·ã,¹ã,³ã§ã¯ã€å¯¾è±¡ãªé™ã,Šæœ€æ–°ã®ã

Cisco IOS Software Checkerã,'ä½¿ç"¨ã™ã,‹ã¨ã€ç‰¹å®šã®Cisco

IOSã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã«å¯¾å¿œã™ã,‹ã,·ã,¹ã,³ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƒªã,
https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.xã«ã,ã,‹Cisco
Security(SIO)ãƒ•ãƒ¼ã,¿ãƒ«ã§ã§å^©ç"¨ã§ã••ã¾ã™ã€,

ãƒ¡ã,¸ãƒ£ãƒ¼ ãƒªãƒªãƒ¼ã,¹	ä¿®æ£æ¸ˆã¿ãƒªãƒªãƒ¼ã,¹ã®å…¥æ‰‹å¯¯èƒ½æ€§
Affected 12.0-Based Releases	**First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã€Ÿæœ€å^ã®ã®ãƒªãƒªãƒ¼ã,¹ï
è©²å½“ã™ã,‹ 12.0 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹ã¯ã,ã,Šã¾ã›ã,"ã€,	
Affected 12.2-Based Releases	**First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã€Ÿæœ€å^ã®ã®ãƒªãƒªãƒ¼ã,¹ï
å½±éŸ¿ã,'å—ã'ã,‹ 12.2 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹ã¯ã,ã,Šã¾ã›ã,"ã€,	
Affected 12.3-Based Releases	**First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã€Ÿæœ€å^ã®ã®ãƒªãƒªãƒ¼ã,¹ï
è©²å½“ã™ã,‹ 12.3 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹ã¯ã,ã,Šã¾ã›ã,"ã€,	
Affected 12.4-Based Releases	**First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã€Ÿæœ€å^ã®ã®ãƒªãƒªãƒ¼ã,¹ï
è©²å½“ã™ã,‹ 12.4 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹ã¯ã,ã,Šã¾ã›ã,"ã€,	
å½±éŸ¿ã,'å—ã'ã,‹ 15.0 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹	**First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã€Ÿæœ€å^ã®ã®ãƒªãƒªãƒ¼ã,¹ï
å½±éŸ¿ã,'å—ã'ã,‹ 15.0 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹ã¯ã,ã,Šã¾ã›ã,"ã€,	
å½±éŸ¿ã,'å—ã'ã,‹ 15.1 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹	**First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã€Ÿæœ€å^ã®ã®ãƒªãƒªãƒ¼ã,¹ï
15.1EY	è„†å¼±æ€§ã®ãªã—
15.1GC	è„†å¼±æ€§ã®ã,Šï¼^ãƒªãƒªãƒ¼ã,¹15.1Mã®æœ€å^ã«ä¿®æ£ï¼‰ 15.1(2)GC2ã,^ã,Šå‰ã®ãƒªãƒªãƒ¼ã,¹ã¯å½±éŸ¿ã,'å—ã'ã¾ã
15.1M	15.1(4)M7 15.1(4)M4ã,^ã,Šå‰ã®ãƒªãƒªãƒ¼ã,¹ã¯å½±éŸ¿ã,'å—ã'ã¾ã›ã
15.1MR	è„†å¼±æ€§ã®ãªã—
15.1S	è„†å¼±æ€§ã®ãªã—
15.1SG	è„†å¼±æ€§ã®ãªã—
15.1SNG	è„†å¼±æ€§ã®ãªã—
15.1SNH	è„†å¼±æ€§ã®ãªã—
15.1T	è„†å¼±æ€§ã®ãªã—
å½±éŸ¿ã,'å—ã'ã,‹ 15.2 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹	**First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã€Ÿæœ€å^ã®ã®ãƒªãƒªãƒ¼ã,¹ï
å½±éŸ¿ã,'å—ã'ã,‹ 15.2 ãƒ™ãƒ¼ã,¹ã®ãƒªãƒªãƒ¼ã,¹ã¯ã,ã,Šã¾ã›ã,"ã€,	
å½±éŸ¿ã,'å—ã'ã,‹ 15.3	**First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã€Ÿæœ€å^ã®ã®ãƒªãƒªãƒ¼ã,¹ï

ãƒ™ãƒ¼ã‚¹ãƒªãƒªãƒ¼ã‚¹
å½±éŸ¿ã‚’å—ã‘ã‚‹ 15.3 ãƒ™ãƒ¼ã‚¹ãƒªãƒªãƒ¼ã‚¹ã¯ã‚ã‚Šã¾ã›ã‚“ã€‚

ä¸€æ£åˆ©ç”¨äº‹ä¾‹ã¨å…¬å¼ç™ºè¡¨

Cisco Product Security Incident Response
Teamï¼ˆPSIRTï¼‰ã¯ã€æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã«è¨˜è¼‰ã•ã‚Œã¦

ã“ã®è„†å¼±æ€§ã¯ã€ŠåŠ¢æ§˜ã®ã‚µãƒãƒ¼ãƒˆã‚±ãƒ¼ã‚¹ã®è§£æ±ºéç¨‹ã§ç™ºè¦‹ã•ã‚Œã¾ã—ãŸã€‚

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131106-sip

æ”¹è¨‚å±¥æ´

ãƒªãƒ“ã‚¸ãƒ§ãƒ³ 1.1	2013å¹´11月15æ—¥	ã€Œå›žé¿ç–€ã€ã®ã€ŒSIPãƒªã‚¯ã‚¨ã‚¹ãƒˆã®ç„¡å
ãƒªãƒ“ã‚¸ãƒ§ãƒ³ 1.0	2013å¹´11月6æ—¥	åˆ©å›žå…¬é–‹ãƒªãƒªãƒ¼ã‚¹

åˆ©ç”¨è¦ç´„

æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã¯ã€ã®ã¨ãŠã‚Šæ¸¡ã•ã‚Œã¦ã„ã¾ã™ã€‚ã
æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã®æƒ…å ±ã‚Šã€ˆã³ã‚ãƒªãƒ³ã‚¯ã®åˆ©ç”¨ã¯ã€è²¬ä»»ã»ã¤ã¦ã€ã
ã¾ãŸã€·ã‚¹ãƒ†ãƒ³ã¯æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã®å†…å®¹ã‚’ã°ˆå‘Šã‚ãªã—ã«å¤‰æ›´ã—ã
æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã®è¨˜è¿°å†…å®¹ã«é–¢ã—ã¦æƒ…å ±é…ä¿¡ã® URL
ã‚’çœç•¥ã—ãŸã€ã‚‚ã—ãã¯æ„図ã‚’æ–½ã—ãŸã‚Šå ´åˆã€å½“社ã¯ç®¡ç
ã“ã®ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã®æƒ…å ±ã¯ã€ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ã‚’å¯¾è±¡

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。