Cisco IOS Software Smart Install Denial of Service Vulnerability

Advisory ID: cisco-sa-20130327-smartinstall

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall/

æ—¥æœ¬èªžã«ã‚ˆã‚‹å ±å‘Šæ–‡ã¯ã€è‹±èªžã«ã‚ˆã‚‹åŽŸæ–‡ã®é€žå…¬å¼ã«ã¤ã¿ã§ã

Revision 1.3

Last Updated 2013 April 11 15:42 UTC (GMT)

For Public Release 2013 March 27 16:00 UTC (GMT)

ç›®æ¬¡

è¦�ç´„

Cisco IOS ã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ã®ã‚¹ãƢãƼãƈ
ã‚¤ãƳã‚¹ãƈãƼãƫæ©Ÿèƒ½ã«ã¯ã¨¨è„†å¼±æ€§ã€Œå˜åœ¨ã™ã‚‹ã€ã€€è¨¼ã•ã‚Œã¦¦

ã‚¹ãƢãƼãƈ ã‚¤ãƳã‚¹ãƈãƼãƫ
ã‚¯ãƩã‚¤ã‚¢ãƳãƈã¨¨ã—ã¦¦è¨å®šã•ã‚Œã¦¦ã„ã‚‹ãƦãƒ•ã‚¤ã‚¹ã¨¨è„†å¼±æ€§ã®å½±éŸ¿ã‚

ã‚·ã‚¹ã¯ã¨“ã®è„†å¼±æ€§ã«å¯¾å‡¦ã™ã‚‹ç„¡å„Ÿã®ã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢
ã‚¢ãƥãƣã‚¯ãƦãƪãƼã‚¹ã‚’æ‰€æœ‰ã—ã¦¦ã„ã‚‹ã¨¨ã«ã¤ã¿ã€ã‚¹ãƢãƼãƈ
ã‚¤ãƳã‚¹ãƈãƼãƫæ©Ÿèƒ½ã‚’æœ‰åŠ¹ã«ã—ã¦¦ã„ã‚‹ã¨¨ã«ã¯ã€ã¨“ã®

ã"ã®ã,¢ãƒ‰ãƒ¬ã,¤ã,¶ãƒªã¯¯ã€æ¬¡ã®ãƪãƳã,¯å…ˆã§ç¢ºèªã§ã§ã¾ã™ã€,

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall/

æ³¨ï¼š2013 å¹´ 3 æœˆ 27 æ—¥ã® Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ã,»ã,ãƒ¥ãƪãƆ†ã,£
ã,¢ãƒ‰ãƒ¬ã,¤ã,¶ãƪ ãƒ«ãƳ‰ãƒ«å…¬é–‹ã«ã¯¯ã€7 ä»¶ã®ã,»ã,ãƒ¥ãƪãƆ†ã,£
ã,¢ãƒ‰ãƒ¬ã,¤ã,¶ãƪã•Œå«ã¾ã,Œã¦ã„ã¾ã™ã€,ã"ã,Œã‚‰ã®ã,¢ãƒ‰ãƒ¬ã,¤ã,¶ãƪã
IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®è„†å¼±æ€§ã«å¯¾å‡¦ã™ã,‹ã,,ã®ã§ã™ã€,å„ Cisco IOS
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ã,»ã,ãƒ¥ãƪãƆ†ã,£
ã,¢ãƒ‰ãƒ¬ã,¤ã,¶ãƪã«ã¯¯ã€ã••ã•®ã,¢ãƒ‰ãƒ¬ã,¤ã,¶ãƪã§è©³è¿°ã••ã,Œã•Ÿè„†å¼±æ€§
Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƪãƪãƪ¼ã,¹ã€ã•Šã,^ã•³ 2013 å¹´ 3
æœˆã«ãƒ‰ãƳ‰ãƒ«å…¬é–—ã•Ÿã•™ã•¹ã•¦ã•® Cisco IOS
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®è„†å¼±æ€§ã,'ä¿®æ£ã™ã,‹ Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
ãƪãƪãƪ¼ã,¹ã,'è¨˜è¼‰ã•—ã•¦ã•„ã•¾ã•™ã€,

å€‹å^¥ã•®å…¬é–‹ãƪãƳã,¯ã•¯ã€•æ¬¡ã•®ãƪãƳã,¯ã•«ã•,ã,‹ã€ŒCisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publicationã€•ã•«æŽ²è¼‰ã••ã,Œã•¦ã•„ã•¾ã•™ã€,

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

è©²å½“è£½å“

è„†å¼±æ€§ã•Œèª•ã,•ã,‰ã,Œã,‹è£½å“

è©²å½“ã•™ã,‹ Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®ã,¹ãƒžãƒ¼ãƒˆ
ã,¤ãƳã,¹ãƒˆãƒ¼ãƫ«æ©Ÿèƒ½ã,'有åŠ¹ã•«ã•—ã•¦ã•„ã,‹ã,·ã,¹ã,³
ãƫãƒ•ã,¤ã,¹ã•«è„†å¼±æ€§ã•Œç"Ÿã•˜ã•¾ã•™ã€,

Cisco IOS ãƒ‡ãƒ•ã,¤ã,¹ã•§ã,¹ãƒžãƒ¼ãƒˆ
ã,¤ãƳã,¹ãƒˆãƒ¼ãƫ«æ©Ÿèƒ½ã•Œæœ‰åŠ¹ã•«ã••ã,Œã•¦ã•„ã,‹ã•‹ã•©ã•†ã•‹ã,'ç¢ºèªã•™ã,‹ã
ã,¤ãƳã,¹ãƒˆãƒ¼ãƫ« ã,¯ãƒ©ã,¤ã,¢ãƳãƒˆã•§ **show vstack config** ç‰¹æ¨© EXEC
ã,³ãƒžãƳãƉ‰ã,'ä½¿"¨ã•—ã•¾ã•™ã€,ã,¹ãƒžãƒ¼ãƒˆ ã,¤ãƳã,¹ãƒˆãƒ¼ãƫ«
ã,¯ãƒ©ã,¤ã,¢ãƳãƒˆã•¨ã•—ã•¦è¨å®šã••ã,Œã•¦ã•„ã,‹ Cisco Catalyst
ã,¹ã,¤ãƒƒãƒ•ã•§å®Ÿè¡Œã•—ã•Ÿ **show vstack config**
ã,³ãƒžãƳãƉ‰ã•®å‡ºåŠ›ã,'æ¬¡ã•«ç¤ºã•—ã•¾ã•™ã€,

```
switch#show vstack config   Role: Client  Vstack Director IP address: 10.1.1.100
```

æ³¨ï¼šã,¹ãƒžãƒ¼ãƒˆ ã,¤ãƳã,¹ãƒˆãƒ¼ãƫ«æ©Ÿèƒ½ã•¯ã€•Cisco IOS

ã,¹ã,¤ãƒƒãƒ•ã�§ã�¯ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã�§æœ‰åŠ¹ã�«ã�ªã�£ã�¦ã�„ã�¾ã�™ã€,

æ³¨ï¼šã,¹ãƒžãƒ¼ãƒˆ ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«
ãƒ‡ã,£ãƒ¬ã,¯ãƒ,ã,¿ã�¨ã�—ã�¦è¨å®šã•ã,Œã�¦ã�„ã,‹ã,·ã,¹ã,³
ãƒ‡ãƒ•ã,¤ã,¹ã�¯ã€•ã•“ã•®è„†å¼±æ€§ã•®å½±éŸ¿ã,’å•—ã•‘ã•¾ã•›ã,“ã€, **show vstack config** ã,³ãƒžãƒ³ãƒ‰ã•®å‡ºåŠ›ã•® *Role: Client* ã•¯ã€•ãƒ‡ãƒ•ã,¤ã,¹ã•§ã,¹ãƒžãƒ¼ãƒˆ ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«æ©Ÿèƒ½ã•Œæœ‰åŠ¹ã•«ã•ªã•£ã•¦ã•„ã,‹ã•“ã•¨ã,’ç¤ºã•—ã•¾ã•™ã€,

ã,·ã,¹ã,³è£½å“•ã•§ç¨¼åƒ•ã•—ã•¦ã•„ã,‹ Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã,¹ã,’ç¢ºèª•ã•™ã,‹ã•«ã•¯ã€•ãƒ‡ãƒ•ã,¤ã,¹ã•«ãƒã,°ã,¤ãƒ³ã•— **show version** ã,³ãƒžãƒ³ãƒ‰ã,’å®Ÿè¡Œã•—ã•¦ã,·ã,¹ãƒ†ãƒ ãƒ•ãƒŠãƒ¼ã,’è¡¨ç¤ºã••ã•›ã•¾ã•™ã€,ã€ŒInternetwork Operating System Softwareã€•ã€•ã€ŒCisco IOS Softwareã€•ã•,ã,‹ã•„ã•¯ã•“ã,Œã,‰ã•«é¡žä¼¼ã•™ã,‹ã,·ã,¹ãƒ†ãƒ ãƒ•ãƒŠãƒ¼ã•«ã,^ã•£ã•¦ãƒ‡ãƒ•ã,¤ã,¹ã•§ Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•Œç¨¼åƒ•ã•—ã•¦ã•„ã,‹ã•“ã•¨ã,’ç¢ºèª•ã•§ã••ã•¾ã•™ã€,ã••ã•®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•Œã•ªã•„å ´å•ˆã,„ã€•è¡¨ç¤ºã•Œç•°ã•ªã,‹å ´å•ˆã•Œã•,ã,Šã•¾ã•™ã€,

æ¬¡ã•®ä¾‹ã•¯ã€•ã,·ã,¹ã,³è£½å“•ã•§ Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã,¹ 15.0(1)M1 ã•Œç¨¼åƒ•ã••ã€•ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ã••ã,Œã•¦ã•„ã,‹ã,¤ãƒ¡ãƒ¼ã,¸å••ã•Œ C3900-UNIVERSALK9-M ã•§ã•,ã,‹ã•“ã•¨ã,’ç¤ºã•—ã•¦ã•„ã•¾ã•™ã€,

<#root>

Router>

show version

```
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE (f
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
```

!--- output truncated

Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®ãƒªãƒªãƒ¼ã,¹å'½å••è¦•å‰‡ã•®è¿½åŠ æƒ…å ±ã•¯ä»¥ä¸‹ã•®ãƒªãƒ³ã,¯ã•«ã Paper: Cisco IOS and NX-OS Software Reference Guideã€•ã•§ç¢ºèª•ã•§ã••ã•¾ã•™ã€,http://www.cisco.com/web/about/security/intelligence/ios-ref.html

è„†å¼±æ€§ã•Œèª•ã,•ã,‰ã,Œã•ªã•„è£½å“•

Cisco IOS XR
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•¯ã€•ã•“ã•®è„†å¼±æ€§ã•®å½±éŸ¿ã,’å•—ã•‘ã•¾ã•›ã,“ã€,

Cisco IOS XE
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•¯ã€•ã•“ã•®è„†å¼±æ€§ã•®å½±éŸ¿ã,’å•—ã•‘ã•¾ã•›ã,“ã€,

ã•“ã•®è„†å¼±æ€§ã•®å½±éŸ¿ã,’å•—ã•‘ã,‹ä»–ã•®ã,·ã,¹ã,³è£½å“•ã•¯ã€•ç•¾åœ¨ç¢ºèª•ã•

è©³ç´°

Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®ã,¹ãƒžãƒ¼ãƒˆ
ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƫ«æ©Ÿèƒ½ã•¯ã€•æ–°ã•—ã•„ã,¹ã,¤ãƒƒãƒ•ã•®ã,¼ãƫã,¿ãƒƒãƒ•å°Žå…¥ã,’å•¯èƒ½

Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®ã,¹ãƒžãƒ¼ãƒˆ
ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƫ«æ©Ÿèƒ½ã•«ã•¯è„†å¼±æ€§ã•Œå˜åœ¨ã•™ã,‹ã•Ÿã,•ã€•èª•è¨¼ã••ã,Œã•¦
ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƫ«æ©Ÿèƒ½ã•¯ã€•é€šä¿¡ã•« TCP ãƒ•ãƒ¼ãƒˆ 4786
ã,’ä½¿ç”¨ã•—ã•¦ã•„ã•¾ã•™ã€,ã•“ã•®è„†å¼±æ€§ã,’ä¸•æ£å^©ç”¨ã•™ã,‹ã•«ã•¯ã€•TCP
ã,¹ãƪãƼã,¦ã,§ã,¤ ãƒ•ãƳãƉ‰ã,·ã,§ã,¤ã,¯ã,’ä½¿ç”¨ã•—ã•¦ TCP
æŽ¥ç¶šã,’ç¢ºç«‹ã•™ã,‹å¿…è¦•ã•Œã•,ã,Šã•¾ã•™ã€,

ã•“ã•®è„†å¼±æ€§ã•¯ã€•ã,¤ãƦãƼã,¸ ãƪã,¹ãƈ
ãƒ©ãƦãƼã,¿ã•®ä¸•æ£å‡¦ç•†ã•«èµ·å› ã•—ã•¾ã•™ã€,æ”»æ’ƈè€…ã•¯ã€•å·§å¦™ã•«ç´°å·¥
ã,¤ãƳ,¹ãƈãƼãƫ« ãƒ‘ã,±ãƫãƈã,’ TCP ãƒ•ãƼãƈ 4786
ã•«é€•ä¿¡ã•™ã,‹ã•“ã•¨ã•§ã€•ã•“ã•®è„†å¼±æ€§ã,’ä¸•æ£å^©ç”¨ã•™ã,‹ã•“ã•¨ã•Œã•§ã
Catalyst ã,¹ã,¤ãƫãƒ•ã•ŒãƪãƫãƼã‰ã••ã,Œã€•ã••ã•®çµ•果ã•¨ã•—ã•¦ DoS
çŠ¶æ…‹ã•«ã•ªã,‹å•¯èƒ½æ€§ã•Œã•,ã,Šã•¾ã•™ã€,

ã•“ã•®è„†å¼±æ€§ã•¯ã€•Cisco Bug ID CSCub55790ï¼ˆç™»éŒ²ãƦãƼã,¶å°‚ç”¨ï¼‰ã•¨ã•—ã•¦æ–‰å›žã••ã,Œã€•Common Vulnerabilities and Exposuresï¼ˆCVEï¼‰ID ã•¨ã•—ã•¦ CVE-2013-1146 ã•Œå‰²ã,Šå½“ã•¦ã,‰ã,Œã•¦ã•„ã•¾ã•™ã€,

è„†å¼±æ€§ã,¹ã,³ã,¢è©³ç´°

ã,·ã,¹ã,³ã•¯æœ¬ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƪã•§ã•®è„†å¼±æ€§ã•«å¯¾ã•—ã€•Common Vulnerability Scoring Systemï¼ˆCVSSï¼‰ã•«åŸºã•¥ã•„ã•Ÿã,¹ã,³ã,¢ã,’æ••ä¾›ã•—ã•¦ã•„ã•¾ã•™ã€,æœ¬ã,»ã,ãƫ
ã,¢ãƫãƒ•ã,¤ã,¶ãƪã•§ã•® CVSS ã,¹ã,³ã,¢ã•¯ã€•CVSS ãƒ•ãƼã,¸ãƫãƳ 2.0
ã•«åŸºã•¥ã•„ã•¦ã•„ã•¾ã•™ã€,

CVSS
ã•¯ã€•è„†å¼±æ€§ã•®é‡•è¦•åº¦ã,’ç¤ºå”†ã•™ã,‹ã,,ã•®ã•§ã€•ç·Šæ€¥æ€§ã•Šã,^ã•³å¯¾å¿œ

ã,·ã,¹ã,³ã€§ã€¯ã€åŸºæœ¬è©•ä¾¡ã,¹ã,³ã,¢ï¼ˆBase
Scoreï¼‰ã€Šã,ˆã€³ç€¾çŠ¶è©•ä¾¡ã,¹ã,³ã,¢ï¼ˆTemporal
Scoreï¼‰ã,'æ€€ä¾›ã€—ã€¦ã€„ã€¾ã€™ã€‚ã€Šå®¢æ§˜ã€¯ã€“ã,Œã,‰ã,'ç"¨ã€„ã€¦ç'ºå¢ƒè©
Scoreï¼‰ã,'ç®—å‡ºã€—ã€€è‡ªèº«ã€®ãƒ€ãƒƒã‚·ãƒ¥ãƒœãƒ¼ãƒ‰ã€«ã€Šã'ã,‹è„†å¼±æ€§ã€®å½±éŸ

ã,·ã,¹ã,³ã€¯æ¬¡ã€®ãƒªãƒ³ã,¯ã€§ CVSS
ã€«é–¢ã€™ã,‹è¿½åŠ æƒ…å ±ã,'æ€€ä¾›ã€—ã€¦ã€„ã€¾ã€™ã€‚

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

ã€¾ã€Ÿã,·ã,¹ã,³ã€§ã€¯ã€€å€„ãƒ€ãƒƒã‚·ãƒ¥ãƒœãƒ¼ãƒ‰ã€«ã€Šã'ã,‹ç'ºå¢ƒå½±éŸ¿åº¦ã,'ç®—å‡ºã€™
CVSS è¨ˆç®—ãƒ„ãƒ¼ãƒ«ã,'æ¬¡ã€®ãƒªãƒ³ã,¯ã€§æ€€ä¾›ã€—ã€¦ã€„ã€¾ã€™ã€‚

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCub55790-- Cisco Smart Install denial of service vulnerability **Calculate the environmental score of**					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

å½±éŸ¿

ã€“ã€®è„†å¼±æ€§ã€Œæ,ªç"¨ã€•ã,Œã,‹ã€¨ã€€è©²å½“ã€™ã,‹ãƒ‡ãƒã,¤ã,¹ã€Œå†€èµ·å‹•ã€™
DoS çŠ¶æ…‹ã€¨ã€ªã,‹å¯¯èƒ½æ€§ã€Œã€,ã,Šã€¾ã€™ã€‚

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒ€ãƒ¼ã,¸ãƒ§ãƒ³ã€Šã,^ã€³ä¿®æ£

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,'æ¤œè¨Žã€™ã,‹å ´å€^ã€¯ã€€http://www.cisco.com/g
ã€® Cisco Security Advisories, Responses, and Notices
ã,¢ãƒ¼ã,«ã,¤ãƒ–ã,„ã€€å¾Œç¶šã€®ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒªã,'å€,ç…§ã€—ã€¦ã€€è¡·ã€“ã,Šã€†ã,‹é
ã,½ãƒªãƒ¥ãƒ¼ã,·ãƒ§ãƒ³ã,'ç¢ºèª€ã€—ã€¦ã€€ã€•ã€„ã€,

ã€„ã€šã,Œã€®å ´å€^ã,,ã€€ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã€™ã,‹ãƒ‡ãƒ€ã,¤ã,¹ã€«å€€å^†ã€ªãƒ¡ãƒ¢ã
Technical Assistance
Centerï¼^TACï¼‰ã,,ã€—ã€€ã€¯å¥'ç´„ã€—ã€¦ã€„ã,‹ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹
ãƒ—ãƒãƒ€ã,¤ãƒ€ãƒ¼ã€«ã€Šå•€ã€„å^ã,€ã€›ã€€ã€•ã€„ã€,

Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒ†ãƒ¼ãƒ–ãƒ«ï¼^ä¸‹è¨˜ï¼‰ã€®å€„è¡Œã€¯ Cisco IOS
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
ãƒˆãƒ¬ã,¤ãƒ³ã,'ç¤ºã€—ã€¾ã€™ã€,ã€,ã,‹ãƒˆãƒ¬ã,¤ãƒ³ã€Œè„†å¼±æ€§ã,'å€«ã,€å ´å€^ã€€ä¿®æ£ã
Fixed Releaseã€€å^—ã€«ç¤ºã€•ã,Œã€¾ã€™ã€,ã€ŒFirst Fixed Release for All Advisories
in the March 2013 Bundled Publicationã€€å^—ã€¯ã€€Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒª
ãƒ€ãƒ³ãƒ‰ãƒ«å…¬é–‹ã€«è¨˜è¼‰ã€•ã,Œã€Ÿã€™ã€¹ã€¦ã€®è„†å¼±æ€§ã,'ä¿®æ£ã€™ã,‹æœ€å

Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒ€ã,§ãƒƒã,«ãƒ¼ã,'å^©ç"¨ã€—ã€¦ã€€ç‰¹å®šã€® Cisco IOS
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã,¹ã€«å¯¾å¿œã€—ã€Ÿã,·ã,¹ã,³ã€®ã,»ã,ãƒ¥ãƒªãƒ†ã,£
ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒªã,'æ¤œç´¢ã€™ã,‹ã€“ã€¨ã€Œã€§ã€€ã€¾ã€™ã€,ã€“ã€®ãƒ„ãƒ¼ãƒ«ã€¯æ
Cisco Security Intelligence
Operationsï¼^SIOï¼‰ãƒ€ãƒ¼ã,¿ãƒ«ã€§å^©ç"¨ã€§ã€€ã€¾ã€™ã€,http://tools.cisco.com/security/cen

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2013 Bundled Publication
There are no affected 12.0 based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 2013 Bundled Publication
12.2	Not vulnerable	Not vulnerable
12.2B	Not vulnerable	Not vulnerable
12.2BC	Not vulnerable	Not vulnerable
12.2BW	Not vulnerable	Not vulnerable
12.2BX	Not vulnerable	Not vulnerable
12.2BY	Not vulnerable	Not vulnerable
12.2BZ	Not vulnerable	Not vulnerable
12.2CX	Not vulnerable	Not vulnerable
12.2CY	Not vulnerable	Not vulnerable

12.2CZ	Not vulnerable	Not vulnerable
12.2DA	Not vulnerable	Not vulnerable
12.2DD	Not vulnerable	Not vulnerable
12.2DX	Not vulnerable	Not vulnerable
12.2EU	Not vulnerable	Not vulnerable
12.2EW	Not vulnerable	Vulnerable; First fixed in Release 12.2SG Releases up to and including 12.2(20)EW4 are not vulnerable.
12.2EWA	Not vulnerable	Vulnerable; First fixed in Release 12.2SG Releases up to and including 12.2(20)EWA4 are not vulnerable.
12.2EX	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(53)EX are not vulnerable.	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(37)EX are not vulnerable.
12.2EY	Vulnerable; migrate to any release in 15.1EY Releases up to and including 12.2(53)EY are not vulnerable.	Vulnerable; First fixed in Release 15.2S
12.2EZ	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(53)EZ are not vulnerable.	Vulnerable; First fixed in Release 15.0SE
12.2FX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FY	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2FZ	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2IRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IRI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2IXA	Not vulnerable	Not vulnerable
12.2IXB	Not vulnerable	Not vulnerable
12.2IXC	Not vulnerable	Not vulnerable
12.2IXD	Not vulnerable	Not vulnerable
12.2IXE	Not vulnerable	Not vulnerable
12.2IXF	Not vulnerable	Not vulnerable
12.2IXG	Not vulnerable	Not vulnerable
12.2IXH	Not vulnerable	Not vulnerable
12.2JA	Not vulnerable	Not vulnerable

12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Not vulnerable
12.2MC	Not vulnerable	Not vulnerable
12.2MRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2S	Not vulnerable	Vulnerable. Only releases 12.2(25)S through 12.2(25)S15 are vulnerable
12.2SB	Not vulnerable	12.2(33)SB12
12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2SCA	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCB	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCC	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCD	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCE	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCF	Not vulnerable	12.2(33)SCF4
12.2SCG	Not vulnerable	Not vulnerable
12.2SCH	Not vulnerable	Not vulnerable
12.2SE	Releases up to and including 12.2(54)SE are not vulnerable. First fixed in: 12.2(55)SE7	12.2(55)SE7 Releases up to and including 12.2(54)SE4 are not vulnerable.
12.2SEA	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEB	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEC	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SED	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEE	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEF	Not vulnerable	Vulnerable; First fixed in Release 15.0SE
12.2SEG	Not vulnerable	Releases prior to 12.2(25)SEG4 are vulnerable; Releases 12.2(25)SEG4 and later are not vulnerable. First fixed inRelease 15.0SE
12.2SG	Not vulnerable	12.2(53)SG9
12.2SGA	Not vulnerable	Vulnerable; First fixed in Release 12.2SG
12.2SM	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SO	Not vulnerable	Not vulnerable
12.2SQ	Not vulnerable	12.2(50)SQ5
12.2SRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	Not vulnerable	12.2(33)SRE8
12.2STE	Not vulnerable	Not vulnerable
12.2SU	Not vulnerable	Not vulnerable

12.2SV	Not vulnerable	Vulnerable. Only releases 12.2(25)SV2, 12.2(27)SV5 and 12.2(29)SV3 are vulnerable.
12.2SVA	Not vulnerable	Not vulnerable
12.2SVC	Not vulnerable	Not vulnerable
12.2SVD	Not vulnerable	Not vulnerable
12.2SVE	Not vulnerable	Not vulnerable
12.2SW	Not vulnerable	Vulnerable; First fixed in Release 15.0M * Releases up to and including 12.2(23)SW1 are not vulnerable.
12.2SX	Not vulnerable	Not vulnerable
12.2SXA	Not vulnerable	Not vulnerable
12.2SXB	Not vulnerable	Not vulnerable
12.2SXD	Not vulnerable	Not vulnerable
12.2SXE	Not vulnerable	Not vulnerable
12.2SXF	Not vulnerable	Not vulnerable
12.2SXH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
12.2SXI	Not vulnerable	12.2(33)SXI11
12.2SXJ	Not vulnerable	12.2(33)SXJ5
12.2SY	Not vulnerable	12.2(50)SY4
12.2SZ	Not vulnerable	Not vulnerable
12.2T	Not vulnerable	Not vulnerable
12.2TPC	Not vulnerable	Not vulnerable
12.2WO	Not vulnerable	Not vulnerable
12.2XA	Not vulnerable	Not vulnerable
12.2XB	Not vulnerable	Not vulnerable
12.2XC	Not vulnerable	Not vulnerable
12.2XD	Not vulnerable	Not vulnerable
12.2XE	Not vulnerable	Not vulnerable
12.2XF	Not vulnerable	Not vulnerable
12.2XG	Not vulnerable	Not vulnerable
12.2XH	Not vulnerable	Not vulnerable
12.2XI	Not vulnerable	Not vulnerable
12.2XJ	Not vulnerable	Not vulnerable
12.2XK	Not vulnerable	Not vulnerable
12.2XL	Not vulnerable	Not vulnerable
12.2XM	Not vulnerable	Not vulnerable
12.2XNA	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNB	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNC	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XND	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability

12.2XNE	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XNF	Please see Cisco IOS XE Software Availability	Please see Cisco IOS XE Software Availability
12.2XO	Not vulnerable	Releases prior to 12.2(54)XO are vulnerable; Releases 12.2(54)XO and later are not vulnerable. First fixed inRelease 12.2SG
12.2XQ	Not vulnerable	Not vulnerable
12.2XR	Not vulnerable	Not vulnerable
12.2XS	Not vulnerable	Not vulnerable
12.2XT	Not vulnerable	Not vulnerable
12.2XU	Not vulnerable	Not vulnerable
12.2XV	Not vulnerable	Not vulnerable
12.2XW	Not vulnerable	Not vulnerable
12.2YA	Not vulnerable	Not vulnerable
12.2YC	Not vulnerable	Not vulnerable
12.2YD	Not vulnerable	Not vulnerable
12.2YE	Not vulnerable	Not vulnerable
12.2YK	Not vulnerable	Not vulnerable
12.2YO	Not vulnerable	Not vulnerable
12.2YP	Not vulnerable	Not vulnerable
12.2YT	Not vulnerable	Not vulnerable
12.2YW	Not vulnerable	Not vulnerable
12.2YX	Not vulnerable	Not vulnerable
12.2YY	Not vulnerable	Not vulnerable
12.2YZ	Not vulnerable	Not vulnerable
12.2ZA	Not vulnerable	Not vulnerable
12.2ZB	Not vulnerable	Not vulnerable
12.2ZC	Not vulnerable	Not vulnerable
12.2ZD	Not vulnerable	Not vulnerable
12.2ZE	Not vulnerable	Not vulnerable
12.2ZH	Not vulnerable	Not vulnerable
12.2ZJ	Not vulnerable	Not vulnerable
12.2ZP	Not vulnerable	Not vulnerable
12.2ZU	Not vulnerable	Not vulnerable
12.2ZX	Not vulnerable	Not vulnerable
12.2ZY	Not vulnerable	Not vulnerable
12.2ZYA	Not vulnerable	Not vulnerable
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**
There are no affected 12.4 based releases		
Affected 15.0-	**First Fixed Release**	**First Fixed Release for All Advisories in the**

Based Releases		March 2013 Bundled Publication
15.0EB	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0ED	Not vulnerable	Not vulnerable
15.0EY	Not vulnerable	Not vulnerable
15.0M	Not vulnerable	15.0(1)M10 *
15.0MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.0S	Not vulnerable	Vulnerable; First fixed in Release 15.1S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SE	15.0(2)SE1	15.0(2)SE1
15.0SG	Not vulnerable	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SQA	Not vulnerable	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	Not vulnerable	15.0(1)SY4
15.0XA	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.0XO	Not vulnerable	Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**
15.1EY	Not vulnerable	Vulnerable; First fixed in Release 15.2S
15.1GC	15.1(4)GC1	15.1(4)GC1
15.1M	Not vulnerable	15.1(4)M6
15.1MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1S	Not vulnerable	** See footnote Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed

		Software section of this advisory.
15.1SNI	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SVA	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.1SVC	Not vulnerable	Not vulnerable
15.1SY	15.1(1)SY1; Available on 24-MAY-13	15.1(1)SY1; Available on 24-MAY-13
15.1T	Not vulnerable	Vulnerable; First fixed in Release 15.1M
15.1XB	Not vulnerable	Vulnerable; First fixed in Release 15.1M
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**
15.2GC	Vulnerable; migrate to any release in 15.4T	Vulnerable; migrate to any release in 15.4T
15.2GCA	Vulnerable; migrate to any release in 15.4T	Vulnerable; migrate to any release in 15.4T
15.2JA	Releases prior to 15.2(2)JA are vulnerable; Releases 15.2(2)JA and later are not vulnerable.	15.2(2)JA
15.2JAX	Not vulnerable	Not vulnerable
15.2JB	Not vulnerable	Not vulnerable
15.2JN	Not vulnerable	Not vulnerable
15.2M	Not vulnerable	15.2(4)M3
15.2S	Not vulnerable	15.2(4)S2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.2SA	Not vulnerable	15.2(2)SA
15.2SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in Obtaining Fixed Software section of this advisory.
15.2SNI	Not vulnerable	Not vulnerable
15.2T	Not vulnerable	15.2(1)T4; Available on 03-MAY-13 15.2(2)T3 15.2(3)T3
Affected 15.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March 2013 Bundled Publication**
15.3S	Not vulnerable	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.3T	Not vulnerable	15.3(1)T1; Available on 29-MAR-13 15.3(2)T; Available on 29-MAR-13

* Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã,¹ 15.0M ã¯ã€2013 å¹´ 4 æœˆ 1 æ—¥ã«ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã‚¹ãƒªãƒªãƒ¼ã‚¹ã•ã‚Œã¦ã„ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’ç¢ºèª
IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã‚¹ 15.1M
ã€ã€®ç§»è¡Œã‚’æ¤œè¨Žã€€ã€•ã€„ã€‚

â€ Cisco 7600 ã,·ãƒªãƒ¼ã,ºã€®ãƒ«ãƒ¼ã,¿ç”¨ã€®æœ€å^€ã€®ä¿®æ£ãƒªãƒªãƒ¼ã‚¹ã€¯ Cisco
IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã‚¹ 15.1(3)S5 ã€§ã€€2013 å¹´ 3 æœˆ ã€® Cisco IOS
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒª
ãƒ€ãƒ³ãƒ‰ãƒ«å…¬é–‹ã€«è¨˜è¼‰ã€•ã,Œã¾ã™ã€‚Cisco 7200 ã€Šã,^ã€³ 7300
ã,·ãƒªãƒ¼ã,ºã€®ãƒ«ãƒ¼ã,¿ç”¨ã€®æœ€å^€ã€®ä¿®æ£ãƒªãƒªãƒ¼ã‚¹ã€¯ Cisco IOS
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã‚¹ 15.1(3)S5a ã€§ã€€2013 å¹´ 3 æœˆ ã€® Cisco IOS
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒª
ãƒ€ãƒ³ãƒ‰ãƒ«å…¬é–‹ã€«è¨˜è¼‰ã€•ã,Œ 2013 å¹´ 4 æœˆ 15
æ—¥ã€«å…¬é–‹ã,’äºˆå®šã€—ã€¦ã€„ã€¾ã€™ã€‚

Cisco IOS XE ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

Cisco IOS XE
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€¯ã€€ã€“ã€®ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒªã€§è¤‡æ˜Žã€•ã,Œã€¦ã€„ã,‹è„†å¼±æ€§ã€

Cisco IOS XR ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

Cisco IOS XR
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€¯ã€€ã€“ã€®ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒªã€§è¤‡æ˜Žã€•ã,Œã€¦ã€„ã,‹è„†å¼±æ€§ã€

å›žé¿ç–

ã,¹ãƒžãƒ¼ãƒˆ
ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«æ©Ÿèƒ½ã,’ç„¡åŠ¹ã€«ã€™ã,‹ä»¥å¤–ã€«ã€€ã€“ã€®è„†å¼±æ€§ã,’è»½æ¸›ã€™ã,‹å›
ã,¹ã,¤ãƒƒãƒ€ã€§ã€¯ã€€ã,¹ãƒžãƒ¼ãƒˆ
ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«æ©Ÿèƒ½ã€¯ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã€§æœ‰åŠ¹ã€«ã€ªã€£ã€¦ã€„ã€¾ã€™ã€‚ã,¯ã
ã,¹ã,¤ãƒƒãƒ€ã€§å¿…è¦ã€ªè¨å®šã€¯ã€,ã,Šã€¾ã€›ã,“ã€‚

Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®ç‰¹å®šã€®ãƒ€ãƒ¼ã,¸ãƒ§ãƒ³ã€§ã€¯ã€€ **no vstack**
ã,°ãƒãƒ¼ãƒ€ãƒ« ã,³ãƒ³ãƒ•ã,£ã,®ãƒ¥ãƒ¬ãƒ¼ã,·ãƒ§ãƒ³
ã,³ãƒžãƒ³ãƒ‰ã,’ä½¿ç”¨ã€—ã€¦ã€€ã,¹ãƒžãƒ¼ãƒˆ
ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«æ©Ÿèƒ½ã,’ç„¡åŠ¹ã€«ã€™ã,‹ã€“ã€¨ã€Œã€§ã€€ã€¾ã€™ã€‚ã€“ã€®ã,³ãƒžãƒ
Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®ç‰¹å®šã€®ãƒ€ãƒ¼ã,¸ãƒ§ãƒ³ã€§ã€¯ã€€ã,¹ãƒžãƒ¼ãƒˆ
ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«æ©Ÿèƒ½ã€Œä¸€è¦§ã€ªå´å^ã€«ã€“ã,Œã,’ç„¡åŠ¹ã€«ã€™ã,‹ã€“ã€¨ã€§è„†

ã,¹ãƒžãƒ¼ãƒˆ ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«æ©Ÿèƒ½ã,’ç„¡åŠ¹ã€«ã€—ã€Ÿ Cisco Catalyst
ã,¹ã,¤ãƒƒãƒ€ã€§å®Ÿè¡Œã€—ã€Ÿ **show vstack config**
ã,³ãƒžãƒ³ãƒ‰ã€®å‡ºåŠ›ã,’æ¬¡ã€«ç¤ºã€—ã€¾ã€™ã€‚

```
switch#show vstack config   Role: Client (SmartInstall disabled)  Vstack
```

```
Director IP address: 10.1.1.100
```

æ³¨ï¼šã,¹ãƒžãƒ¼ãƒˆ ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«æ©Ÿèƒ½ã,'ç„¡åŠ¹ã«ã«ã™ã,‹ **no vstack** ã,°ãƒãƒ¼ãƒ«ãƒ« ã,³ãƒ³ãƒ•ã,£ã,®ãƒ¥ãƒ¬ãƒ¼ã,·ãƒ§ãƒ³ ã,³ãƒžãƒ³ãƒ‰ã«¯ã€Cisco Bug CSCtj75729ï¼ˆã€ŒAbility to shut Smart Install default service on TCP port 4786ã€ï¼‰ã«ã«Šã'ã,‹ä¿®æ£ã§å°Žå…¥ã•ã,Œã¾ã—ãŸã€,Cisco IOS ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®ãƒªãƒªãƒ¼ã,¹ã§ã,¹ãƒžãƒ¼ãƒˆ ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«æ©Ÿèƒ½ã•ã,Œã¦ã„ã,‹ã®ã«ã€ **no vstack** ã,³ãƒžãƒ³ãƒ‰ã•Œå˜åœ¨ã—ãªã„å ´å^ã€Cisco Bug CSCtj75729 ã«é–¢ã™ã,‹ä¿®æ£ã•Œå«ã¾ã,Œã¦ã„ã„ã¾ã›ã,“ã€,

ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã,¯å†…ã•®ã,·ã,¹ã,³ ãƒ‡ãƒã,¤ã,¹ã«é©ç”¨å¯èƒ½ãªã••ã••ã•®ä»–ã•®å›žé¿ç–ã«ã¤ã•„ã¦ã¯ã€ä»˜å±žã•™ã,‹ and Mitigating Exploitation of the Cisco IOS Software Smart Install Denial of Service Vulnerabilityã€ã•§ç´¹ä»‹ã—ã•¦ã„ã•¾ã•™ã€,ã•“ã•®ãƒ‰ã,ãƒ¥ãƒ¡ãƒ³ãƒˆã¯ã€æ¬¡ã•®
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=28655/

ä¿®æ£æ¸ˆã•¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®å…¥æ‰‹

ã,·ã,¹ã,³ã•¯ã•“ã•®ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã•«è¨˜è¼‰ã••ã,Œã•Ÿè„†å¼±æ€§ã•«å¯¾å‡¦ã•™ã,‹ç„¡å,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã,'æ••ä¾›ã•—ã•¦ã•„ã•¾ã•™ã€,ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®å°Žå…¥ã,'è¡Œã•†ã•¨ã•—ã•¦ã•„ãƒ—ãƒãƒ•ã,¤ãƒ€ãƒ¼ã•«ã•"ç›¸è«‡ã•„ã•Ÿã• ã••ã•‹ã€•ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®ãƒ•ã,£ãƒ¼ãƒ•ãƒ£ã,»ãƒƒãƒˆã•®äº'æ•›æ€§ã•Šã,^ã•³ã•Šå®¢æ§˜ã•®ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã,¯ç'°å¢ƒã•®ç‰¹æœ‰ã•®

ã•Šå®¢æ§˜ã•Œã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ã•—ã•Ÿã,Šã,µãƒ•ãƒ¼ãƒˆã,'å•—ã•'ã•Ÿã,Šã•§ã••ã,‹ã•®ã,»ãƒƒãƒˆã•«å¯¾ã•—ã•¦ã•®ã•¿ã•¨ã•ªã,Šã•¾ã•™ã€,ã••ã•®ã,^ã•†ã•ªã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,'ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ã€•ãƒ€ã,¦ãƒ³ãƒãƒ¼ãƒ‰ã€•ã,¯ã,»ã,¹ã•¾ã•Ÿã•¯ã
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
ã•«è¨˜è¼‰ã•®ã,·ã,¹ã,³ã•®ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒ©ã,¤ã,»ãƒ³ã,¹ã•®æ•¡é …ã•«å¾“ã•†ã•“ã•¨ã•«å•Œæ„•ã••ã•—ã•Ÿã•“ã•¨ã•«ã•ªã,Šã•¾ã

ã,µãƒ¼ãƒ“ã,¹å¥‘ç´„ã,'ã•”å^©ç”¨ã•®ã•Šå®¢æ§˜

ã,µãƒ¼ãƒ“ã,¹å¥‘ç´„ã,'ã•”å^©ç”¨ã•®ã•Šå®¢æ§˜ã•¯ã€•é€šå„ã•®ã,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆ ãƒ•ãƒ£ãƒ•ãƒ¼ãƒ«ã•‹ã,‰ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,'å…¥æ‰‹ã•—ã•¦ã••ã• ã••ã•„ã€,ã•»ã•¨ã,“ã•©ã•®ã•Šå®¢æ§˜ã•¯ã Cisco.com ã•® Software Navigator ã•‹ã,‰ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,'å…¥æ‰‹ã•§ã••ã•¾ã•™ã€,
http://www.cisco.com/cisco/software/navigator.html

ã,µãƒ¼ãƒ‰ãƒ‘ãƒ¼ãƒ†ã,£ã•®ã,µãƒ•ãƒ¼ãƒˆä¼šç¤¾ã,'ã•”å^©ç”¨ã•®ã•Šå®¢æ§˜

ã,·ã,¹ã,³ ãƒ‘ãƒ¼ãƒˆãƒŠãƒ¼ã€•æ£è¦•è²©å£²ä»£ç•†åº—ã€•ã,µãƒ¼ãƒ“ã,¹ ãƒ—ãƒã,¤ã,¹ã•ªã•©ã€•ã,µãƒ¼ãƒ‰ãƒ‘ãƒ¼ãƒ†ã,£ã•®ã,µãƒ•ãƒ¼ãƒˆä¼šç¤¾ã•¨ä»¥å‰•ã

å›žé•ç–ã,„ä¿®æ£ã•®åŠ¹æžœã•¯ã€•ä½¿ç”¨ã•—ã•¦ã•„ã,‹è£½å“•ã€•ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã,¯

ãƒˆãƒ©ãƒƒã‚¸ãƒ¼ã€ãƒˆãƒ©ãƒ•ã‚£ãƒƒã‚¯ã®æ€§èƒ½ã„çµ„ç¹”ã®ç›®çš„ã®ãªã©ã«é–¢ã™ã‚‹ã
ãƒ—ãƒãƒã‚¤ãƒ€ãƒ¼ã„ã‚µãƒãƒ¼ãƒˆä¼šç¤¾ã«ã”ç¢ºèª ã ã ã• ã•ã„ã€‚

ã‚µãƒ¼ãƒ"ã‚¹å¥'ç´„ã‚'ã"åˆ©ç"¨ã§ãªã„ãŠå®¢æ§˜

ã‚·ã‚¹ã‚³ã‹ã‚‰è£½å"ã‚'ç›´æŽ¥è³¼å…¥ã—ãŸã‚‚ã®ã®ã‚·ã‚¹ã‚³ã®ã‚µãƒ¼ãƒ"ã‚¹å¥'ç´„ã‚'ã"åˆ
ãƒ™ãƒ³ãƒ€ãƒ¼ã‹ã‚‰è³¼å…¥ã—ãŸã‚‚ã®ã®ä¿®æ£æ¸ˆã¿ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã'è³¼å…¥å…ˆã
Technical Assistance Centerï¼ˆTACï¼‰ã«é€£çµ¡ã—ã¦ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰
ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã'å…¥æ‰‹ã—ã¦ã ã ã• ã•ã„ã€‚

- +1 800 553 2447ï¼ˆåŒ—ç±³ã‹ã‚‰ã®ç„¡æ–™é€šè©±ï¼‰
- +1 408 526 7209ï¼ˆåŒ—ç±³ä»¥å¤–ã‹ã‚‰ã®æœ‰æ–™é€šè©±ï¼‰
- E ãƒ¡ãƒ¼ãƒ«ï¼štac@cisco.com

ç„¡å„Ÿã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã®å¯¾è±¡è£½å"ã§ã‚ã‚‹ã"ã¨ã'è¨¼æ˜Žã—ã¦ã„ãŸã
URL
ã'ã"ç"¨æ„ã ã ã• ã•ã„ã€‚ã‚µãƒ¼ãƒ"ã‚¹å¥'ç´„ã'ã"åˆ©ç"¨ã§ãªã„ãŠå®¢æ§˜ã¯
TAC ã«ç„¡å„Ÿã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã'ãƒªã‚¯ã‚¨ã‚¹ãƒˆã—ã¦ã ã ã• ã•ã„ã€‚

å¤šè¨€èªžã«ã‚ˆã‚‹å„åœ°ã®é›»è©±ç•ªå·ã€èª¬æ˜Žã€E ãƒ¡ãƒ¼ãƒ«
ã‚¢ãƒ‰ãƒ¬ã‚¹ãªã©ã® TAC ã®é€£çµ¡å…ˆæƒ…å ±ã«ã¤ã„ã¦ã¯ã€Cisco
Worldwide Contact
ã'å‚ç…§ã—ã¦ã ã ã• ã•ã„ã€‚http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.

ä¸æ£åˆ©ç"¨äº‹ä¾‹ã¨å…¬å¼ç™ºè¡¨

Cisco Product Security Incident Response
Teamï¼ˆPSIRTï¼‰ã§ã¯ã€æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã«è¨˜è¼‰ã•ã‚Œã¦ã„ã‚‹è„†å¼±æ€

ã"ã®è„†å¼±æ€§ã¯ Tenable Network Security
ãƒãƒ¼ãƒ ã«ã‚ˆã£ã¦ç™ºè¦‹ã•ã‚Œã€ZDI
ã‹ã‚‰ã‚·ã‚¹ã‚³ã«å ±å'Šã•ã‚Œã¾ã—ãŸã€‚

ã"ã®é€šçŸ¥ã®ã‚¹ãƒ†ãƒ¼ã‚¿ã‚¹ï¼šFinal

æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã¯ç„¡ä¿è¨¼ã®ã‚‚ã®ã¨ã—ã¦ã"æä¾›ã—ã¦ãŠã‚Šã

å¾Œè¿°ã™ã‚‹æƒ…å ±é…ä¿¡ã® URL
ã'çœç•¥ã—ã€æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã®è¨˜è¿°å†…å®¹ã«é–¢ã—ã¦å˜ç‹¬ã®è»¢

æƒ…å ±é…ä¿¡

ã“ã®ã‚¢ãƒ‰ãƒ“ã‚¤ã‚¶ãƒªãƒ¼ã¯ã€Cisco Security Intelligence Operations ã«æŽ²è¼‰ã•ã‚Œã¾ã™ã€‚

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall/

ã¾ãŸã€“ã®ã‚¢ãƒ‰ãƒ“ã‚¤ã‚¶ãƒªãƒ¼ã®ãƒ†ã‚ã‚¹ãƒˆç‰ˆã€Cisco PSIRT PGP ã‚ãƒ¼ã«ã‚ˆã‚‹ãƒªãƒªãƒ¼ã‚¹å¾Œã«å¤‰æ›´ã•ã‚Œã¦ã„ãªã„ E ãƒ¡ãƒ¼ãƒ«ã§é…ä¿¡ã•ã‚Œã¦ã„ã¾ã™ã€‚

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

æœ¬ã‚¢ãƒ‰ãƒ“ã‚¤ã‚¶ãƒªãƒ¼ã«é–¢ã™ã‚‹æƒ…å ±ã¯ Cisco.com ã«æŽ²è¼‰ã•ã‚Œã¾ã™ã€‚ãƒªãƒ¼ãƒªã‚¹ãƒˆã‚„é…ä¿¡ã•ã‚Œã‚‹ã¨ã¨ã‚‚ã«ã€æ›´æ–°å†…å®¹ã«ã¤ã„ã¦ã¯ URL ã§ç¢ºèªã•ã‚Œã¾ã™ã€‚

æ›´æ–°å±¥æ´

Revision 1.3	2013-April-11	Updated vulnerability status for 15.0EY and 15.0SG trains.
Revision 1.2	2013-March-28	Updated "Software Versions and Fixes" section, corrected software table.
Revision 1.1	2013-March-27	Updated Software Versions and Fixes section.
Revision 1.0	2013-March-27	Initial public release.

ã‚·ã‚¹ã‚³ ã‚»ã‚ãƥãƪãƆã‚£æ‰‹é †

ã‚·ã‚¹ã‚³è£½å“ã«ã‚Šã‘ã‚‹ã‚»ã‚ãƥãƪãƆã‚£ã®è„†å¼±æ€§ã®å ±å‘Šã€ã‚»ã‚ãƥãƪãƆã‚£ä¾µæ ã® http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html ã‚’å‚ç…§ã—ã¦ã€ã“ã®ã‚¢ãƒ‰ãƒ“ã‚¤ã‚¶ãƒªãƒ¼ Web ãƫšãƒ¼ã‚¸ã«ã¨ã‚·ã‚¹ã‚³ã®ãƻ»ã‚ãƥãƪãƆã‚£ã‚¢ã‚¯ã‚»ã‚¹ã€ã‚¢ãƥãƪãƆã‚£ã‚¢ã‚¯ã‚»ã‚¹ã«é–¢ã—ã¦ãƫãƆã‚£ã‚¢ã‚¯ã‚»ã‚¹ã®æŒ‡ç¤ºã«ã“ã®ã‚¢ãƥãƪãƆã‚£ ã‚¢ãƥãƪãƆã‚£ã«ã¤ã„ã¦ã¯ã€ã“ã®ã‚¢ãƥãƪãƆã‚£ã‚¢ã‚¯ã‚»ã‚¹ http://www.cisco.com/go/psirt/ ã§ç¢ºèªã§ã¾ã™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。