Multiple Vulnerabilities in Cisco NX-OS-Based Products

Advisory ID: cisco-sa-20140521-nxos

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-nxos

æ—¥æœ¬èªžã«ã‚ˆã‚‹å ±å‘Šã€è‹±èªžã«ã‚ˆã‚‹åŽŸæ–‡ã®é€žå…¬å¼€ã«ã‚ˆã‚ç¿»è¨³ã§ã‚ã‚Š

Revision 2.3

Last Updated 2014 June 2 20:25 UTC (GMT)

For Public Release 2014 May 21 16:00 UTC (GMT)

ç›®æ¬¡

è¦�ç´„

Cisco Nexusã€Cisco Unified Computing Systemï¼ˆUCSï¼‰ã€ã‚Šã‚ˆã³ Cisco 1000 ã‚·ãƒªãƒ¼ã‚º Connected Grid ãƒ«ãƒ¼ã‚¿ï¼ˆCGRï¼‰ã¯ã™ã¹ã¦ã€Cisco NX-OS ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã‚’å®Ÿè¡Œã—ã¦ã„ã‚‹ã¨ã—ã¦ã„ã‚‹ãƒ‡ãƒã‚¤ã‚¹ã¨ã‚‚ã«ã€ã‚ã‚‰ã‚†ã‚‹è£½å“ã¯ã¯ã€ä¸Žæ¬¡ã®è„†å¼±æ€§ã‚’å—ã‘ã‚‹å¯èƒ½æ€§ãŒã‚ã‚Šã¾ã™ã€‚

- Cisco NX-OS Virtual Device Context ã® SSH ã«ãŠã‘ã‚‹æ¨©é™æ˜‡æ ¼ã®è„†å¼±æ€§
- Cisco NX-OS Virtual Device Context ã® SSH ã‚ãƒ¼ã«ã‚‹æ¨©é™æ˜‡æ ¼ã®è„†å¼±æ€§

- Cisco NX-OS ãƒ™ãƒ¼ã‚¹ã£è£½å“ã®ã® Smart Call Home ã«ãŠã‘ã‚‹ãƒ•ãƒƒãƒ•ã‚¡ã‚ªãƒ¼ãƒãƒ•ãƒãƒ•ãƒ¼ã®è„†å¼±æ€§
- Cisco NX-OS ãƒ¡ãƒƒã‚»ãƒ¼ã‚¸è»¢é€ã‚µãƒ¼ãƒ“ã‚¹ã«ãŠã‘ã‚‹ DoS è„†å¼±æ€§
    - å…¬å¼ãƒªãƒªãƒ¼ã‚¹
      ã‚¤ãƒ¡ãƒ¼ã‚¸ã§ã‚Œã‚‰ã®è„†å¼±æ€§ã‚’å¯¾è±¡ã¨ã—ãŸã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã‚¹ ãƒªãƒªãƒ¼ã‚¹ãŒæ••ä¾›ã—ã¦ã„ã¾ã™ã€‚

ã‚·ã‚¹ãƒ†ãƒ ã®è¨å®šãŒæ¬¡ã®æ¡ä»¶ã«ä¸€è‡´ã™ã‚‹å ´åˆã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’å—ã‘ã¾ã™ã€‚

- ãã‚Œã‚‰ã®è„†å¼±æ€§ã¯ã€ãƒªãƒªãƒ¼ã‚¹ 6.2(2) ã¾ãŸã¯ãã‚Œä»¥é™ã®ãƒªãƒªãƒ¼ã‚¹ã§ã¯ä¿®æ£ã•ã‚Œã¦ã„ã¾ã™ã€‚
- ãã‚Œã‚‰ã®è„†å¼±æ€§ã¯ã€ãƒªãƒªãƒ¼ã‚¹ 7.0(3)I1(1) ã¾ãŸã¯ãã‚Œä»¥é™ã®ãƒªãƒªãƒ¼ã‚¹ã§ã¯ä¿®æ£ã•ã‚Œã¦ã„ã¾ã™ã€‚

ã“ã®ã¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã¯ã€æ¬¡ã®ãƒªãƒ³ã‚¯ã§ç¢ºèªã§ãã¾ã™ã€‚
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-nxos

è©²å½“è£½å“

Cisco NX-OS ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ 6.2(2) ã¾ãŸã¯ãã‚Œä»¥é™ã®ãƒªãƒªãƒ¼ã‚¹ã‚’å®Ÿè¡Œã—ã¦ã„ã‚‹ã€ã‚¹ã‚¤ãƒƒãƒãƒ³ã‚°ãƒ¢ãƒ¼ãƒ‰ã® Cisco Nexus 1 ã¤ä»¥ä¸Šã®å½±éŸ¿ã‚’å—ã‘ã‚‹ã‚·ã‚¹ãƒ†ãƒ ã€‚

è„†å¼±æ€§ã‚’å«ã‚€è£½å“

æ¬¡ã®è£½å“ã«ã¯ã€è„†å¼±æ€§ã‚’å˜ä¸€ã§å«ã‚€ã‚‚ã®ã‚‚ã‚ã‚Šã¾ã™ã€‚

	UCS 6100	UCS 6200	Nexus 9000	Nexus 7000	Nexus 6000	Nexus 5000	Nexus 4000	Nexus 3000	Nexus 1000v	MDS 9000	CGE 100
Cisco NX-OS Virtual Device Context SSH Privilege Escalation Vulnerability CVE-2014-2200				X							
Cisco NX-OS Virtual Device Context SSH Key Privilege Escalation Vulnerability CVE-2013-1191				X							
Cisco NX-OS-Based Products Smart Call Home Buffer Overflow Vulnerability CVE-2014-3261	X	X		X		X	X	X			X

Cisco NX-OS Message Transfer Service Denial of Service Vulnerability CVE-2014-2201 *No Officially Released Versions are Affected*											
Recommended Release	2.2(1d)	2.2(1d)	N/A	6.2(8)	N/A	5.2(1)N1(7) 6.0(2)N2(4) 7.0(2)N1(1)	4.1(2)E1(11)	5.0(3)U5(1) 6.0(2)U2(4)	N/A	N/A	CG4(15.4(1)

å‡¡ä¾‹ï¼š

UCS 6100 = Cisco Unified Computing Server ãƒ•ã,¡ãƒ–ãƒªãƒƒã,¯ ã,¤ãƒ³ã,¿ãƒ¼ã,³ãƒ•ã,¯ãƒˆ 6100 ã,·ãƒªãƒ¼ã,º ãƒ‡ãƒ•ã,¤ã,¹
UCS 6200 = Cisco Unified Computing Server ãƒ•ã,¡ãƒ–ãƒªãƒƒã,¯ ã,¤ãƒ³ã,¿ãƒ¼ã,³ãƒ•ã,¯ãƒˆ 6200 ã,·ãƒªãƒ¼ã,º ãƒ‡ãƒ•ã,¤ã,¹
Nexus 9000 = Cisco Nexus 9000 ã,·ãƒªãƒ¼ã,º ãƒ‡ãƒ•ã,¤ã,¹
Nexus 7000 = Cisco Nexus 7000 ã,·ãƒªãƒ¼ã,º ãƒ‡ãƒ•ã,¤ã,¹
Nexus 6000 = Cisco Nexus 6000 ã,·ãƒªãƒ¼ã,º ãƒ‡ãƒ•ã,¤ã,¹
Nexus 5000 = Cisco Nexus 5000 ã,·ãƒªãƒ¼ã,ºã•Šã,ˆã•³ Cisco Nexus 5500 ã,·ãƒªãƒ¼ã,º ãƒ‡ãƒ•ã,¤ã,¹
Nexus 4000 = Cisco Nexus 4000 ã,·ãƒªãƒ¼ã,º ãƒ–ãƒ¬ãƒ¼ãƒ‰ ãƒ‡ãƒ•ã,¤ã,¹
Nexus 3000 = Cisco Nexus 3000 ã•Šã,ˆã•³ Cisco Nexus 3500 ã,·ãƒªãƒ¼ã,º ãƒ‡ãƒ•ã,¤ã,¹
Nexus 1000V = Cisco Nexus 1000V ã,·ãƒªãƒ¼ã,º ã,¹ã,¤ãƒƒãƒ•ã•Šã,ˆã•³ 1010 ä»®æƒ³ã,µãƒ¼ãƒ“ã,¹ ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹
MDS 9000 = Cisco MDS 9000 ãƒžãƒ«ãƒ•ã•¤ã,¹ã,¤ãƒƒãƒ•/ãƒ‡ã,£ãƒ¬ã,¯ã,¿ ãƒ•ã,¡ãƒŸãƒª ãƒ‡ãƒ•ã,¤ã,¹
CGR 1000 = Cisco 1000 ã,·ãƒªãƒ¼ã,º Connected Grid ãƒ«ãƒ¼ã,¿ ãƒ‡ãƒ•ã,¤ã,¹

æ³¨ï¼šä¸Šã•®è¡¨ã•® Recommended Release ã•«è¨˜è¼‰ã••ã,Œã•Ÿãƒªãƒªãƒ¼ã,¹ã•¯ã€•ä¸Šè¨˜ã•®å•„ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ ã•«å½±éŸ

è„†å¼±æ€§ã•Œèª•ã,•ã,‰ã,Œã•ªã•„è£½å“•

- Cisco Nexus 9000 ã,·ãƒªãƒ¼ã,º
- Cisco Nexus 7700 ã,·ãƒªãƒ¼ã,º
- Cisco Nexus 6000 ã,·ãƒªãƒ¼ã,º
- Cisco Nexus 5600 ã,·ãƒªãƒ¼ã,º
- Cisco Nexus 2000 ã,·ãƒªãƒ¼ã,º
- Cisco Nexus 1000V ã,·ãƒªãƒ¼ã,º
- Cisco Nexus 1010 ã,·ãƒªãƒ¼ã,º ã,¢ãƒ—ãƒªã,±ãƒ¼ã,·ãƒ§ãƒ³ ã,µãƒ¼ãƒ“ã,¹ ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ

- Cisco Nexus 1100 ã,·ãƒªãƒ¼ã,º ã,¯ãƒ©ã,¦ãƒ‰ ãƒ¼ãƒ“ã,¹ ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ
- Cisco MDS 9000 ãƒžãƒ«ãƒ€ãƒ¬ã,¤ãƒ¤ ã,¹ã,¤ãƒƒãƒ€/ãƒ‡ã,£ãƒ¬ã,¯ã,¿ ãƒ•ã,¡ãƒŸãƒª ãƒ‡ãƒ€ã,¤ã,¹

ä»–ã€®ã,·ã,¹ã,³è£½å“€ã€«ã€Šã€„ã€¦ã€“ã€®ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒªã€®å½±éŸ¿ã,’å€—ã€‘ã,‹ã,,

è©³ç´°

Cisco NX-OS Virtual Device Context ã€® SSH ã€«ã€Šã€‘ã,‹æ¨©é™€æ˜‡æ ¼ã€®è„†å¼±æ€§

Cisco NX-OS
ãƒ™ãƒ¼ã,¹ã€®ãƒ‡ãƒ€ã,¤ã,¹ã€«ã€¯æ¨©é™€æ˜‡æ ¼ã€®è„†å¼±æ€§ã€Œå˜åœ¨ã€—ã€¾ã€™ã
ã,³ãƒ³ãƒ†ã,ã,¹ãƒˆï¼ˆVDCï¼‰ã€Œå˜åœ¨ã€—ã€€ã€‹ã€¤ãƒãƒ¼ã,«ãƒ«èª€è¨¼ã€Œè¨®šã€•ã,Œã€
SSH
ã,’é€šã€˜ã€¦ç®¡ç€†ã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã€«ã,¢ã,¯ã,»ã,¹ã€§ã€€ã,‹å ´å€ˆã€€å^¥ã€®
VDC
ã€®ç®¡ç€†è€…æ¨©é™€ã,’å––å¾—ã€—ã€¦èª€è¨¼ã,’é€šé€Žã€™ã,‹å¯¯èƒ½æ€§ã€Œã€,ã,Šã

ã€“ã€®è„†å¼±æ€§ã€¯ã€Cisco Bug ID CSCti11629ï¼ˆç™»éŒ²ãƒ¦ãƒ¼ã,¶ã€®ã€¿ï¼‰ã€¨ã€—ã€¦æ–‡æ›¸åŒ–ã€•ã,Œã€Common Vulnerabilities and Exposuresï¼ˆCVEï¼‰ID CVE-2014-2200 ã€Œå‰²ã,Šå½“ã€¦ã,‰ã,Œã€¦ã€„ã€¾ã€™ã€‚

Cisco NX-OS Virtual Device Context ã€® SSH ã,ãƒ¼ã€«ã,^ã,‹æ¨©é™€æ˜‡æ ¼ã€®è„†å¼±æ€§

Cisco NX-OS
ãƒ™ãƒ¼ã,¹ã€®ãƒ‡ãƒ€ã,¤ã,¹ã€«ã€¯æ¨©é™€æ˜‡æ ¼ã€®è„†å¼±æ€§ã€Œå˜åœ¨ã€—ã€¾ã€™ã
ã,³ãƒ³ãƒ†ã,ã,¹ãƒˆï¼ˆVDCï¼‰ã€Œå˜åœ¨ã€—ã€€ã€‹ã€¤ãƒãƒ¼ã,«ãƒ«èª€è¨¼ã€Œè¨®šã€•ã,Œã€
SSH
ç®¡ç€†ã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã€«ã,¢ã,¯ã,»ã,¹ã€§ã€€ã,‹ãƒªãƒ¢ãƒ¼ãƒˆã€®èª€è¨¼æ¸ˆã€¿æ”»æ’ƒè
ã,ãƒ¼
ãƒ•ã,¡ã,¤ãƒ«ã€®ä¸€éƒ¨ã€¨ã€—ã€¦æ€€ä¾›ã€•ã,Œã,‹ãƒã,°ã,¤ãƒ³æƒ…å ±ã,’æ“€ä½œã€—ã€€ã€
VDC
ã€®ç®¡ç€†è€…æ¨©é™€ã,’å––å¾—ã€§ã€€ã,‹ã,^ã€†ã€«ã€ªã,Šã€¾ã€™ã€,ã€¾ã€Ÿã€€ç‰

ã€“ã€®è„†å¼±æ€§ã€¯ã€Cisco Bug ID CSCud88400ï¼ˆç™»éŒ²ãƒ¦ãƒ¼ã,¶å°,ç”¨ï¼‰ã€¨ã€—ã€¦æ–‡æ›¸åŒ–ã€•ã,Œã€CVE IDã€«ã€CVE-2013-1191 ã€Œå‰²ã,Šå½“ã€¦ã,‰ã,Œã€¦ã€„ã€¾ã€™ã€‚

Cisco NX-OS ãƒ™ãƒ¼ã,¹è£½å“€ã€® Smart Call Home ã€«ã€Šã€‘ã,‹ãƒ€ãƒƒãƒ•ã,¡ ã,ªãƒ¼ãƒ€ãƒ¼ãƒ•ãƒãƒ¼ã€®è„†å¼±æ€§

Smart Call Home

ãƒ•ã‚£ãƒ¼ãƒ‰ãƒ£ ã‚»ãƒƒã‚·ãƒ§ãƒ³ãƒˆã—ã¦ã„ã‚‹ Cisco NX-OS
ãƒ™ãƒ¼ã‚¹ã®è£½å““ã‚’ã¯ãƒãƒƒã•ã¡
ã‚ªãƒ¼ãƒãƒ¼ãƒ•ãƒãƒ¼ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’å—ã‘ã‚‹ã‚‚ã®ã‚‚ã‚ã‚Œã¦ã
SMTP ã‚µãƒ¼ãƒãƒ¼ã®å^¶å¾¡æ¨©é™ã‚’ã‚‚ã–å¾—ã§ã§ã‚‹ã‚‚ã
ã‚ªãƒ¼ãƒãƒ¼ãƒ•ãƒãƒ¼çŠ¶æ…‹ã‚’å¼•ã••è¼·ã““ã›ã‚‹å¯¯èƒ½æ€§ã‚Œã‚‚ã‚ã‚Šã¾ã™ã€‚ã““ã

ã““ã®è„†å¼±æ€§ã¯ã€Smart Call Home ã®é€šçŸ¥ã®é€ä¿¡ä¸ã«ãƒªã‚¯ã‚¨ã‚¹ãƒˆ
ãƒ›ã‚¹ãƒˆã‹ã‚‰å—ä¿¡ã—ãŸå…¥åŠ›ã‚’é©å^‡ã«ã‚µãƒ‹ã‚¿ã‚¤ã‚ºã•ã‚Œã““ã¨

è©²å½“ã™ã‚‹ãƒ‡ãƒã‚¤ã‚¹ãƒ§ãƒ³ã®ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ã‚’å®Ÿè¡Œã—ã¦ã„ã‚‹ã‚·ã‚¹ãƒ†ãƒ ã§ã€
Call Home ã‚’è¨å®šã—ã¦ã„ã‚‹å ´å^ˆã«ã®ã¿ã€SMTP
ãƒ¬ãƒãƒ¼ãƒˆã‚’ä½¿ç”¨ã—ã¦ã„ã‚‹å ´å^ˆã«ã®ã¿è„†å¼±æ€§ã€Œå˜åœ¨ã—ã¾ã™ã

ã““ã®è„†å¼±æ€§ã¯ Cisco Bug ID
ã§æ–‡æ›¸åŒ–ã•ã‚Œã¦ã¾ã™ã€‚

- **Cisco Unified Computing System ãƒ•ã‚¡ãƒ–ãƒªã‚¯ã‚¤ãƒ³ã‚¿ãƒ¼ã‚³ãƒã‚¯ãƒˆ** - CSCtk00695 (ç™»éŒ²ãƒ¦ãƒ¼ã‚¶ãƒ¼å°‚ç”¨)
- **Nexus 3000**ï¼šCSCts56633ï¼ˆç™»éŒ²ãƒ¦ãƒ¼ã‚¶ãƒ¼å°‚ç”¨ï¼‰
- **Nexus 5000**ï¼šCSCts56632ï¼ˆç™»éŒ²ãƒ¦ãƒ¼ã‚¶ãƒ¼å°‚ç”¨ï¼‰
- **Nexus 7000**ï¼šCSCts56628ï¼ˆç™»éŒ²ãƒ¦ãƒ¼ã‚¶ãƒ¼å°‚ç”¨ï¼‰
- **Nexus 4000**ï¼šCSCug14405ï¼ˆç™»éŒ²ãƒ¦ãƒ¼ã‚¶ãƒ¼å°‚ç”¨ï¼‰
- **CG-OS ã€Œç¨¼åƒã€™ã‚‹ Cisco Connected 1000 ã‚·ãƒªãƒ¼ã‚º Connected Grid ãƒ«ãƒ¼ã‚¿** - CSCuf61322ï¼ˆç™»éŒ²ãƒ¦ãƒ¼ã‚¶ãƒ¼å°‚ç”¨ï¼‰

ã““ã®è„†å¼±æ€§ã« CVE ID CVE-2014-3261
ã€Œå‰²ã‚Šå½“ã¦ã¦ã„ã‚‰ã‚Œã¦ã„ã¾ã™ã€‚

Cisco NX-OS ãƒ¡ãƒƒã‚»ãƒ¼ã‚¸è»¢é€ã‚µãƒ¼ãƒ“ã‚¹ã«ãŠã‘ã‚‹ DoS è„†å¼±æ€§

è©³ç´°ã€¨ãƒ³ã‚¸ãƒ‹ã‚¢ãƒªãƒ³ã‚°è¿œæŸ»ã€»é€šã€ˆã‚Šã€å…¬é–‹ãƒªãƒªãƒ¼ã‚¹ã€
ã‚¤ãƒ¡ãƒ¼ã‚¸ã«ã¤ã„ã¦ã¯ã€¯ã¯ã¯ã¯ã€°è¿œæŸ»ã€»é€šã€ˆã‚Šã€å…¬é–‹ãƒªãƒªãƒ¼ã‚¹ã®ã““ã¨ã‚’ç¢ºèªã—ã¦ãã ã•ã„ã€‚
OS 6.0
ã€®å…¬é–‹ãƒªãƒªãƒ¼ã‚¹ã€ã‚‰ã‚Œã¦ã„ãªã„ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã‚¹ãƒªãƒªãƒ¼ã‚¹ã€ã‚‚ã¯ã¯ã¯ã€

Cisco NX-OS ãƒ¡ãƒ¼ã‚¸ãƒ§ãƒ³ 6.0(1)
ã®ãƒ¡ãƒƒã‚»ãƒ¼ã‚¸è»¢é€ã‚µãƒ¼ãƒ“ã‚¹ï¼ˆMTSï¼‰ã«ã‚ã‚‹è„†å¼±æ€§ã«ã‚ˆã£ã¦å½±éŸ¿ã

ã““ã®è„†å¼±æ€§ã¯ã€è©²å½“ãƒ‡ãƒã‚¤ã‚¹ã«ã€Œé›Žå‰°ã€ªè² è·ã«ã•ã‚‰ã•ã‚Œã
NULL
ãƒ¬ãƒ³ã‚¿ãƒ«ã®é€†å¸‚ã§ã«è¨å®šã•ã‚Œã¦ã„ã¾ã™ã€æ”»æ’ƒè€…ã¯ã¯ã€å·¦å¦™ã«ç´°å·¥ã•ã
ãƒ‘ãƒƒãƒ‰ã¯ã€Œå¼•ã••è¼·ã““ã•ã‚Œã€çµæžœçš„ã« DoS
çŠ¶æ…‹ã«è‡³ã‚Šã¾ã™ã€‚

ã“ã®è„†å¼±æ€§ã¯ CSCtw98915ï¼ˆç™»éŒ²ãƒ¦ãƒ¼ã‚¶å°‚ç”¨ï¼‰ã¨ã—ã¦æ–‡æ›¸åŒ–ã•ã‚Œã€CVE ID CVE-2014-2201 ã€Œå‰²ã‚Šå½“ã¦ã¦ã„ã‚‰ã‚Œã¦ã„ã¾ã™ã€‚

è„†å¼±æ€§ã‚¹ã‚³ã‚¢

ã‚·ã‚¹ãƒ†ãƒ ã“ã®è„†å¼±æ€§ã«ã‚ˆã‚Šã€Common Vulnerability Scoring Systemï¼ˆCVSSï¼‰ã«åŸºã¥ã„ã¦ã‚¹ã‚³ã‚¢ãŒä»˜ä¸Žã•ã‚Œã¦ã„ã¾ã™ã€‚æœ¬ã‚»ã‚¯ã‚·ãƒ§ãƒ³ã¯ CVSS ã‚¹ã‚³ã‚¢ CVSS ãƒãƒ¼ã‚¸ãƒ§ãƒ³ 2.0 ã«åŸºã¥ã„ã¦ã„ã¾ã™ã€‚

CVSS ã¯è„†å¼±æ€§ã®é‡è¦åº¦ã‚’ç¤ºå”†ã™ã‚‹ã‚‚ã®ã§ã‚ã‚Šã€ã‚ªãƒšãƒ¬ãƒ¼ã‚·ãƒ§ãƒ³ã‚’ç½®ãæ›ãˆã‚‹ã‚‚ã®ã§ã¯ã‚ã‚Šã¾ã›ã‚“ã€‚ãŠå®¢æ§˜ã¯ã€ç’°å¢ƒã«é–¢é€£ã™ã‚‹è„…å¨ã«åŸºã¥ã„ã¦ã€ã”è‡ªèº«ã®å±é™ºæ€§ã‚’è©•ä¾¡ã™ã‚‹ã“ã¨ã‚’æŽ¨å¥¨ã—ã¾ã™ã€‚

ã‚·ã‚¹ãƒ†ãƒ ã§åˆ©ç”¨å¯èƒ½ãªæ¬¡ã®è„†å¼±æ€§ã‚¹ã‚³ã‚¢ï¼šBase Scoreï¼šã‚ã‚ç´„ã¯ã€Temporal Scoreï¼šæ™‚é–“çµŒéŽã«ã‚ˆã‚‹å¤‰åŒ–ã‚’è€ƒæ…®ã—ãŸã‚¹ã‚³ã‚¢ã€Environmental Scoreï¼šé¡§å®¢ã®ãƒãƒƒãƒˆãƒ¯ãƒ¼ã‚¯ã«ãŠã‘ã‚‹æ½œåœ¨çš„ãªå½±éŸ¿ã«åŸºã¥ãã‚¹ã‚³ã‚¢

ã‚·ã‚¹ãƒ†ãƒ ã§ã¯ CVSS ã«é–¢é€£ã™ã‚‹ä»¥ä¸‹ã®ãƒ‰ã‚ãƒ¥ãƒ¡ãƒ³ãƒˆã‚‚åˆ©ç”¨ã§ãã¾ã™ã€‚ CVSS ã«é–¢ã™ã‚‹ FAQ ã¯ã€æ¬¡ã® URL ã«ã‚ã‚Šã¾ã™ã€‚
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

ã¾ã‚Šã‚·ã‚¹ãƒ†ãƒ ã§ã¯ã€ãƒãƒƒãƒˆãƒ¯ãƒ¼ã‚¯ã«ãŠã‘ã‚‹ç’°å¢ƒå½±éŸ¿åº¦ã‚’ç®—å‡ºã™ã‚‹ CVSS è¨ˆç®—ãƒ„ãƒ¼ãƒ«ã‚’æ¤œè¨¼ã™ã‚‹ã“ã¨ã‚‚ã§ãã¾ã™ã€‚
http://tools.cisco.com/security/center/cvssCalculator.x

Cisco NX-OS Virtual Device Context SSH Privilege Escalation Vulnerability - CSCti11629 **Calculate the environmental score of**					
CVSS Base Score - **7.1**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	Single	Complete	Complete	Complete

CVSS Temporal Score - **5.9**		
Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

Cisco NX-OS Virtual Device Context SSH Key Privilege Escalation Vulnerability - CSCud88400 **Calculate the environmental score of**					
CVSS Base Score - **7.1**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	Single	Complete	Complete	Complete
CVSS Temporal Score - **5.9**					
Exploitability	Remediation Level	Report Confidence			
Functional	Official-Fix	Confirmed			

Cisco NX-OS-Based Products Smart Call Home Buffer Overflow Vulnerability - CSCtk00695, CSCts56633, CSCts56632, CSCts56628, CSCuf61322, CSCug14405 **Calculate the environmental score of**

CVSS Base Score - **7.6**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	Complete	Complete	Complete
CVSS Temporal Score - **6.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

Cisco NX-OS Message Transfer Service Denial of Service Vulnerability - CSCtw98915 **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¿

Cisco NX-OS Virtual Device Context ã�® SSH
ã�«ã�Šã�'ã,‹æ¨©é™�æ˜‡æ ¼ã�®è„†å¼±æ€§ã�¾ã�Ÿã�¯ Cisco NX-OS Virtual Device Context ã�® SSH
ã,ãƒ¼ã�«ã,^ã,‹æ¨©é™�æ˜‡æ ¼ã�®è„†å¼±æ€§ã�®ä¸�æ£å^©ç"¨ã�«æ^�åŠŸã�—ã�Ÿå ´å�^ã€
VDC
ã�¸ã�®ã,¢ã,¯ã,»ã,¹æ¨©é™�ã,'å�–å¾—ã�§ã��ã,‹å�¯èƒ½æ€§ã�Œã�,ã,Šã�¾ã�™ã€,

Cisco NX-OS ãƒ™ãƒ¼ã,¹è£½å“�ã�® Smart Call Home ã�«ã�Šã�'ã,‹ãƒ�ãƒƒãƒ•ã,¡
ã,ªãƒ¼ãƒ�ãƒ¼ãƒ•ãƒƒãƒ¼ã�®è„†å¼±æ€§ã�®ä¸�æ£å^©ç"¨ã�«æ^�åŠŸã�—ã�Ÿå ´å�^ã€�æ"»æ'ƒè

Cisco NX-OS ãƒ¡ãƒƒã,»ãƒ¼ã,¸è»¢é€�ã,µãƒ¼ãƒ"ã,¹ã�«ã�Šã�'ã,‹ DoS
è„†å¼±æ€§ã�®ä¸�æ£å^©ç"¨ã�«æ^�åŠŸã�—ã�Ÿå ´å�^ã€�æ"»æ'ƒè€…ã�Œè©²å½"ãƒ‡ãƒ�ã,¤ã
DoS
çŠ¶æ…‹ã,'ç"Ÿã�˜ã�•ã�›ã,‹å�¯èƒ½æ€§ã�Œã�,ã,Šã�¾ã�™ã€,å ´å�^ã�«ã,^ã�£ã�¦ã�¯ã€�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/go/psirt/ 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�„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
Centerï¼ˆTACï¼‰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�„ã€,

Cisco Unified Computing Systemï¼š
Cisco NX-OS ãƒ™ãƒ¼ã,¹è£½å“�ã�® Smart Call Home ã�«ã�Šã�'ã,‹ãƒ�ãƒƒãƒ•ã,¡
ã,ªãƒ¼ãƒ�ãƒ¼ãƒ•ãƒƒãƒ¼ã�®è„†å¼±æ€§

Affected Version	First Fixed Release	Recommended Release
1.0	N/A	2.2(1d)
1.1	N/A	2.2(1d)
1.2	N/A	2.2(1d)
1.3	N/A	2.2(1d)
1.4(1h) and prior	1.4(1i)	2.2(1d)

Cisco Nexus 7000ï¼š
Cisco NX-OS Virtual Device Context ã�® SSH ã�«ã�Šã�'ã,‹æ¨©é™�æ˜‡æ ¼ã�®è„†å¼±æ€§

Affected Version	First Fixed Release>	Recommended Release

4.X	N/A	6.2(8)
5.0(2a) and prior	5.0(5)	6.2(8)

Cisco NX-OS Virtual Device Context ã€® SSH ã‚ãƒ¼ã€«ã‚ˆã‚‹æ¨©é™€æ˜‡æ ¼ã€®è„†å¼±æ€§

Affected Version	First Fixed Release	Recommended Release
4.X	N/A	6.2(8)
5.X	N/A	6.2(8)
6.0	N/A	6.2(8)
6.1(4a) and prior	6.1(5)	6.2(8)

Cisco NX-OS ãƒ™ãƒ¼ã‚¹ã€®è£½å“ã€® Smart Call Home ã€«ã€Šã€‘ã‚‹ãƒ€ãƒƒã•ã‚¡ã‚¹ãƒ•ã‚¡ã‚¤ãƒ«ã€®è„†å¼±æ€§

Affected Version	First Fixed Release	Recommended Release
4.X	N/A	6.2(8)
5.0	N/A	6.2(8)
5.1	N/A	6.2(8)
5.2(3) and prior	5.2(3a)	6.2(8)

Cisco Nexus 5000ï¼š
Cisco NX-OS ãƒ™ãƒ¼ã‚¹ã€®è£½å“ã€® Smart Call Home ã€«ã€Šã€‘ã‚‹ãƒ€ãƒƒã•ã‚¡ã‚¹ãƒ•ã‚¡ã‚¤ãƒ«ã€®è„†å¼±æ€§

Affected Version	First Fixed Release	Recommended Release
4.X	N/A	5.2(1)N1(7) 6.0(2)N2(4) 7.0(2)N1(1)
5.0	5.1(3)N1(1)	5.2(1)N1(7) 6.0(2)N2(4) 7.0(2)N1(1)

Cisco Nexus 4000ï¼š
Cisco NX-OS ãƒ™ãƒ¼ã‚¹ã€®è£½å“ã€® Smart Call Home ã€«ã€Šã€‘ã‚‹ãƒ€ãƒƒã•ã‚¡ã‚¹ãƒ•ã‚¡ã‚¤ãƒ«ã€®è„†å¼±æ€§

Affected Version	First Fixed Release	Recommended Release
4.1(2)E1(1k) and prior	4.1(2)E1(1l)	4.1(2)E1(1l)

Cisco Nexus 3000ï¼š
Cisco NX-OS ãƒ™ãƒ¼ã‚¹ã€®è£½å“ã€® Smart Call Home ã€«ã€Šã€‘ã‚‹ãƒ€ãƒƒã•ã‚¡ã‚¹ãƒ•ã‚¡ã‚¤ãƒ«ã€®è„†å¼±æ€§

Affected Version	First Fixed Release	Recommended Release
5.0(3)U2(1) and prior	5.0(3)U2(2)	5.0(3)U5(1j)

		6.0(2)U2(4)

Cisco 1000 ã,·ãƒªãƒ¼ã,º Connected Grid ãƒ«ãƒ¼ã,¿ï¼š
Cisco NX-OS ãƒ™ãƒ¼ã,¹è£½å“�ã�® Smart Call Home ã�«ã�Šã�'ã,‹ãƒ�ãƒƒãƒ•ã,¡
ã,ªãƒ¼ãƒ�ãƒ¼ãƒ•ãƒãƒ¼ã�®è„†å¼±æ€§

Affected Version	First Fixed Release	Recommended Release
CG3	N/A	CG4(3) 15.4(1)CG
CG4(1)	CG4(2)	CG4(3) 15.4(1)CG

å›žé�¿ç–

å›žé�¿ç–ã�¯ã�,ã,Šã�¾ã�›ã,"ã€,

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

ã,·ã,¹ã,³ã�¯ã�"ã�®ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�«è¨˜è¼‰ã�•ã,Œã�Ÿè„†å¼±æ€§ã�«å¯¾å‡¦ã�™ã,‹ç„¡
ã,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã,'æ��ä¾›ã�—ã�¦ã�„ã�¾ã�™ã€,ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®åº Žå…¥ã,'è¡Œã�†
ãƒ—ãƒãƒ�ã,¤ãƒ€ãƒ¼ã�«ã�"ç›¸è«‡ã�„ã�Ÿã� ã��ã�‹ã€�ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ãƒ•ã,£ãƒ¼ãƒ�ã
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
ã,»ãƒƒãƒˆã«å¯¾ã�—ã�¦ã�®ã�¿ã�¨ã�ªã,Šã�¾ã�™ã€,ã��ã�®ã,^ã�†ã�ªã,½ãƒ•ãƒˆã,¦ã,§ã,
ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,'ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ã€�ãƒ€ã,¦ãƒ³ãƒãƒ¼ãƒ‰ã€�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�¨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�ãƒ«ã�‹ã,‰ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,'å…¥æ‰‹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,'å…¥æ‰‹ã™ã,‹ã"ã¨¨ã,Œã§ã��ã¾ã™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—ãƒãƒ¤ãƒ¼ã,¤ãƒ€ãƒ¼ã,µãƒ¼ãƒ‰ãƒ'ãƒ¼ãƒ†ã,£ã,µãƒ¼ãƒ“ã,¹ãƒ—ãƒãƒ¤ãƒ¼ã,¤ãƒ€ãƒ¼ã,'ã»¥å‰ã

å›žé¿ç–ã‚„ä¿®æ£ã®åŠ¹æžœã¯ã€ä½¿ç”¨ã—ã—ã¦ã„ã‚‹è£½å“ã€ãƒãƒƒãƒˆãƒ¯ãƒ¼ã‚¯ã€
ãƒˆãƒ©ãƒ•ã‚£ãƒƒã‚¯ã€ãƒ©ã‚¤ãƒ•ã‚¹ã‚¿ã‚¤ãƒ«ã€ã‚µãƒ¼ãƒ“ã‚¹ã«ã‚ˆã£ã¦ç°ãªã‚Šã¾ã™ã€‚

ã‚µï¼ãƒ“ã‚¹ãƒ¬ãƒ™ãƒ«ã‚’é¸æŠžã—ãªã„å®¢æ§˜

ã‚·ã‚¹ãƒ†ãƒ ã‚’é›¾å…¥ã…¥ã—ã¦ã„ãŸã‚Šã€ã‚¯ãƒªãƒ†ã‚£ã‚«ãƒ«ãªãƒ“ã‚¸ãƒã‚¹ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³ã‚’
Technical Assistance Centerï¼ˆTACï¼‰ã«é€£çµ¡ã—ã¦ã‚‚ã‚ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰
ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã‚’å…¥æ‰‹ã—ã¦ã„ãŸã ã‘ã¾ã›ã‚“ã€‚

- +1 800 553 2447ï¼ˆç„¡æ–™é€šè©±ï¼‰
- +1 408 526 7209ï¼ˆç±³å›½å¤–ã‹ã‚‰ã®æœ‰æ–™é€šè©±ï¼‰
- Eãƒ¡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„ã€
URL
ã‚’ã”ç”¨æ„ã„ãŸã ã•ã„ã€‚ãµãƒ¼ãƒ“ã‚¹ã‚’ã”åˆ©ç”¨ã«ãªã„ãŠå®¢æ§˜ã¯
TAC ã«ç„¡å„Ÿã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã‚’ãƒªã‚¯ã‚¨ã‚¹ãƒˆã—ãªã„ã§ãã ã•ã„ã€‚

ã•ã¾ã–ã¾ãªè¨€èªžå‘ã‘ã®å„„åœ°ã®é›»è©±ç•ªå·€ã€€èª¬æ˜Žã€€é›»å¡ãƒ¼ãƒ«ã‚¢ãƒ‰ãƒ¬ã‚¹ã€ã‚¦ã‚§ãƒ–ãƒã‚¤ãƒˆã€ã‚¯ãƒ©ã‚¤ã‚¢ãƒ³ãƒˆ TAC
ã®é€£çµ¡å…ˆæƒ…å ±ã«ã¤ã„ã¦ã¯ã€ã€Œã€ã‚ã‚¤ãƒ³ã‚¿ãƒ¼ãƒãƒƒãƒˆã§ã‚µãƒãƒ¼ãƒˆã‚’å—ã‘ã‚‹æ–¹æ³•ã€ã€
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.htmlï¼‰ã‚’å‚ç…§ã—ã¦ã„ãŸã ã

ä¸€æ£åˆ©ç”¨ä°‹ä¾‹ã¨å…¬å¼€ç™ºè¡¨

Cisco Product Security Incident Response
Teamï¼ˆPSIRTï¼‰ã§ã¯ã€ã‚·ã‚¹ãƒ†ãƒ ã‚¤ãƒ¶ãƒ¥ãƒªãƒ†ã‚£ã«é¢¨ã™ã‚‹è„†å¼±æ€§

ã“ã‚Œã‚‰ã®è„†å¼±æ€§ã¯ã€ã‚·ã‚¹ãƒ†ãƒ ç¤¼å†…ã§ã®ã¿ç¢ºèªã•ã‚Œã¦ã„ã¾ã™ Cisco
TAC ã«ã‚ˆã‚‹ã€ãƒžãƒ¼ã‚±ãƒ†ã‚£ãƒ³ã‚°ä¸Šã®ç™ºè¡¨ã«ã¯ã€ã‚Œã¾ã—ãŸã€‚

ã“ã®é€šçŸ¥ã®ãƒãƒ¼ã‚¸ãƒ§ãƒ³å±¥æ´

ãƒãƒ¼ã‚¸ãƒ§ãƒ³	èª¬æ˜Ž	æ—¥ä»˜
1.0	åˆå›žå…¬é–‹ãƒªãƒªãƒ¼ã‚¹	2019 å¹´ 3 æœˆ 27 æ—¥

æƒ…å ±é…ä¿¡

ã“ã®é€šçŸ¥ã®æœ€æ–°ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã¯ Cisco Security Intelligence

Operations ã«æŽ²è¼‰ã•ã‚Œã¾ã™ã€‚
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-nxos

ã¾ã Ÿã€ã“ã®ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªãƒ†ã‚£ã‚’ã‚ˆã‚Š Cisco PSIRT PGP ã‚ãƼã«ã‚ˆã‚‹ã¯ã‚ç½²å••ã•ã¤ã¤ã§ã‚‚æ¬¡ã®é›»å•ãƒ¡ãƼãƫã«é…•ä¿¡ã•ã‚Œã¦ã¦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‚ƒãƒ‰ãƒã‚¤ã‚¶ãƫã«é–¢ã™ã‚‹æƒ…å ±ã¯ Cisco.com ã«æŽ²è¼‰ã•ã‚Œã¾ã™ã€‚ãƫãƼãƫãƳã€‚ ãƫã‚¹ãƈã§é…•ä¿¡ã•ã‚Œã‚‹ã¨ã¯é™•ã‚Šã¾ã›ã‚“ã€‚æ›´æ–°å†…å®¹ã«ã¤ã„ã¦ã¯ã€ã¾ã¦ã¯ URL ã§ã”ç¢ºèªã•ã•ã• ã•ã„ã€‚

æ›´æ–°å±¥æ´

Revision 2.3	2014-June-02	Updated Recommended Version in Nexus 7000 Software tables for the Cisco NX-OS Virtual Device Context SSH Privilege Escalation Vulnerability to match other tables.
Revision 2.2	2014-May-29	Removed Nexus 5500UP devices from the Confirmed Not Vulnerable section.While these devices shipped with a non-vulnerable version of NX-OS, they are capable of running an affected version of 5.0(3).
Revision 2.1	2014-May-28	Added a clarifying statement to the Smart Call Home vulnerability to stipulate that SCH must be configured to utilize SMTP as the reporting method.
Revision 2.0	2014-May-28	Further engineering efforts have determined that no officially released images are affected by the Message Transfer Service Denial of Service vulnerability.Customers running a pre-release version of NX-OS 6.0 may be affected and are advised to update to an official release.MDS 9000 Family moved to Products Confirmed Not Vulnerable.
Revision 1.1	2014-May-21	Updated tables for legibility purposes.
Revision 1.0	2014-May-21	Initial public release.

ã,·ã,¹ã,³ ã,»ã,ãƒ¥ãƒªãƒ†ã,£æ‰‹é †

ã,·ã,¹ã,³è£½å“ï¿½ã«ã€Šã‘ã,‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã®è„†å¼±æ€§ã®å ±å‘Šã€ã,»ã,ãƒ¥ãƒªãƒ†ã,£äº‹æ
ã® http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html
ã,’å,ç…§ã—ã¦ã••ã„ã€‚ã“ã® Web
ãƒšãƒ¼ã,¸ã«ã¯ã€·ã,¹ã,³ã®ã,»ã,ãƒ¥ãƒªãƒ†ã,£
ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã«é–¢ã—ã¦ãƒ¡ãƒ‡ã,£ã,¢ã€Œå•ï¿½ã„å‚ã,ï¿½ã›ã,‹éš›ã®æŒ‡ç¤ºã€Œ
ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã¯ã€ http://www.cisco.com/go/psirt/
ã§ç¢ºèªï¿½ã™ã,‹ã“ã¨ã€Œã§ã••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。