Cisco Anomaly Detection and Mitigationè£½å“�ã�«ã�Šã�‘ã‚‹TACACS+èª�è¨

severity

ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªãƒ¼ID : cisco-sa-20060215-guard
åˆ�å…¬é–‹æ—¥ : 2006-02-15 16:00
ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ 1.1 : Final
å›žé�¿ç– : No Workarounds available
Cisco ãƒ�ã‚° ID :

[CVE-2006-0764](CVE-2006-0764)

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

æ¦‚è¦�

Cisco Anomaly Detection and Mitigation(ANOMALY)ã‚¢ãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹ã�Šã‚ˆã�³ã‚µãƒ¼ãƒ“ã‚¹ãƒ¢ã‚¸ãƒ¥ãƒ¼ãƒ«ã�§ä½¿ç”¨ã�•ã‚Œ Access Controller Access Control System Plus(TACACS+)ã�®è¨å®šã�Œä¸�å®Œå…¨ã�ªå ´å�ˆã€�ä¸�æ£ãƒ¦ãƒ¼ã‚¶ã�Œãƒ‡ãƒ�ã‚¤ã‚¹ã�«

TACACS+èª�è¨¼ã�¯ãƒ‡ãƒ•ã‚©ãƒ«ãƒˆã�§ç„¡åŠ¹ã�«ã�ªã�£ã�¦ã�Šã‚Šã€�TACACS+èª�è¨¼ç”¨ã�

ã‚·ã‚¹ã‚³ã�§ã�¯ã€�è©²å½“ã�™ã‚‹ã�Šå®¢æ§˜ç”¨ã�«ã€�ã�“ã�®è„†å¼±æ€§ã�«å¯¾å¿œã�™ã‚‹

ã�“ã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�¯ã€�[https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityA sa-20060215-guard](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityA) ã�§å…¬é–‹ã�•ã‚Œã�¦ã�„ã�¾ã�™ã€‚

è©²å½“è£½å“�

ã�“ã�®ã‚»ã‚¯ã‚·ãƒ§ãƒ³ã�«ã�¯ã€�è©²å½“è£½å“�ã�«é–¢ã�™ã‚‹è©³ç´°ã�ŒæŽ²è¼‰ã�•ã‚Œã�

è„†å¼±æ€§ã�®ã�‚ã‚‹è£½å“�

ã�“ã�®è„†å¼±æ€§ã�¯ã€�Cisco Guardã�Šã‚ˆã�³Cisco Traffic Anomaly Detectorã‚¢ãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹ç”¨ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã�®ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³5.0(1)ã�Šã‚ˆã�³5.0(3)ã Catalyst 6500ã‚¹ã‚¤ãƒƒãƒ�/Cisco 7600ãƒ«ãƒ¼ã‚¿ç”¨Anomaly Guardãƒ¢ã‚¸ãƒ¥ãƒ¼ãƒ«ã�Šã‚ˆã�³Traffic Anomaly Detectorãƒ¢ã‚¸ãƒ¥ãƒ¼ãƒ«ã�«å½±éŸ¿ã�—ã�¾ã�™ï¼ˆãƒ‡ãƒ�ã‚¤ã‚¹ã�ŒTACACS+èª�è¨¼ã‚’ä½¿ç

è©²å½“ã�™ã‚‹ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã�Œç¨¼åƒ�ã�—ã€�TACACS+èª�è¨¼ã�Œè¨å

Authorization, and Accounting(AAA)ã,³ãƒžãƒ³ãƒ‰ã�§TACACS+èª�è¨¼ã�ŒæŒ‡å®šã�•ã,Œã�¦ã�„ã�¦ã,,ã€�TAC **server host**ã,³ãƒžãƒ³ãƒ‰ã�Œè¨å®šã�•ã,Œã�¦ã�„ã�ªã�„å ´å�ˆã�«è„†å¼±ã�§ã�™ã€,ã�¤ã�¾ã,Šã�

```
aaa authentication login tacacs+ local
aaa authentication enable tacacs+ local
```

ã�Ÿã� ã�—ã€�æ¬¡ã�®ã,³ãƒžãƒ³ãƒ‰ã�¯*ã�,ã,Šã�¾ã�›ã,“*ã€,

```
tacacs-server host <IP address of TACACS+ server>
```

ãƒ‡ãƒ�ã,¤ã,¹ã�«è„†å¼±æ€§ã�Œå˜åœ¨ã�—ã�¾ã�™ã€,

æ³¨ï¼šä¸Šè¨˜ã�®aaa authenticationã,³ãƒžãƒ³ãƒ‰ã�§ã€Œtacacs+ã€�èª�è¨¼æ–¹å¼�ã�®å¾Œã�«æŒ‡å®šã�•ã,Œã� **server host**ã,³ãƒžãƒ³ãƒ‰ã�Œã�ªã�„å ´å�ˆã€�ã€Œãƒãƒ¼ã,«ãƒ«ã€�èª�è¨¼æ–¹å¼�ã�®æœ‰ç„¡ã�«ã

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

Cisco Guardã�Šã,ˆã�³Cisco Traffic Anomaly Detectorã�¯ã€�æ¬¡ã�®ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ã,’å®Ÿè¡Œã�—ã�¦ã�„ã,‹å ´å�ˆã�

- Cisco Guardã�Šã,ˆã�³Cisco Traffic Anomaly Detectorã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®5.0ã,ˆã,Šå‰�ã�®ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ã€,ã�“ã,Œã�«ã�¯ã€�
- Cisco Guardã�Šã,ˆã�³Cisco Traffic Anomaly Detectorã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³5.1ä»¥é™�ã€,

Cisco Guardã�¾ã�Ÿã�¯Cisco Traffic Anomaly Detectorã�Œãƒ�ãƒ¼ã,¸ãƒ§ãƒ³5.0(1)ã�¾ã�Ÿã�¯5.0(3)ã,’å®Ÿè¡Œã�—ã�¦ã�„ã,‹å ´å�ˆã€�ãƒ‡ã **server host**ã,³ãƒžãƒ³ãƒ‰ã�Œå�«ã�¾ã,Œã�¦ã�„ã,‹å ´å�ˆ)ã�¯å½±éŸ¿ã,’å�—ã�‘ã�¾ã�›ã,“ã€,

æ³¨ï¼š TACACS+**èª**�è¨¼ã�¯ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã�§ç„¡åŠ¹ã�«ã�ªã�£ã�¦ã�„ã�¾ã�™ã€,æ˜Žç¤ºçš„ã�ªA Guardã�¨Cisco Traffic Anomaly

Detectorã�¯ãƒãƒ¼ã,«ãƒ«ãƒ‡ãƒ¼ã,¿ãƒ™ãƒ¼ã,¹ï¼ˆã€Œãƒãƒ¼ã,«ãƒ«ã€�èª�è¨¼æ–¹å¼�ï¼‰ã�«å¯¾

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

è©³ç´°

Cisco Guardã�Šã,ˆã�³Cisco Traffic Anomaly Detectorã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã€�ã�ªã,‰ã�³ã�«Cisco Catalyst 6500ã,¹ã,¤ãƒƒãƒ�/Cisco 7600ãƒ«ãƒ¼ã,¿ç”¨ã�®Anomaly Guard Moduleã�Šã,ˆã�³Traffic Anomaly Detector Moduleã�¯ã€�åˆ†æ•£åž‹Denial of Service(DDoS)æ”»æ'ƒã�®ç·©å'Œãƒ‡ãƒ�ã,¤ã,¹ã�§ã�,ã,Šã€�æ½œåœ¨çš„ã�ªDDoSæ”»æ'ƒã�®å˜å

Cisco Guardã�Šã,ˆã�³Cisco Anomaly Traffic Detectorã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã�¯ã€�ä»®æƒ³ç«¯æœ«ï¼ˆã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã�«ç›´æŽ¥æŽ¥ç¶š Catalyst 6500ã,¹ã,¤ãƒƒãƒ�/Cisco 7600ãƒ«ãƒ¼ã,¿ç”¨ã�®Anomaly Guardãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«ã�Šã,ˆã�³Traffic Anomaly Detectorãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«ã�¯ã€�ã,¹ã,¤ãƒƒãƒ�ã�‹ã,‰(**session**ã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç”¨ã�—ã�¦)ãƒ¢ã,¸ãƒ

TACACS+ã�¯ã€�ã,µãƒ¼ãƒ�ã€�ãƒ¯ãƒ¼ã,¯ã,¹ãƒ†ãƒ¼ã,·ãƒ§ãƒ³ã€�ãƒ«ãƒ¼ã,¿ã€�ã,¹ã,¤ãƒƒãƒ�ã€�ã,¢

Cisco Guardã�Šã,ˆã�³Cisco Anomaly Traffic Detectorãƒ‡ãƒ�ã,¤ã,¹ã�«ã,¢ã,¯ã,»ã,¹ã�™ã,‹ãƒ¦ãƒ¼ã,¶ã�¯ã€�ãƒ‡ãƒ�ã,¤ã,¹ã�®è¨å®šã�«ä¿�å˜ã

```
aaa authentication login tacacs+ local
aaa authentication enable tacacs+ local

tacacs-server host <IP address of TACACS+ server>
```

aaa authentication login tacacs+ã,³ãƒžãƒ³ãƒ‰ã�¯ã€�SSHã�¾ã�Ÿã�¯Webã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã,'ä»‹ã�—ã�¦ãƒ‡ãƒ�ã,¤ã **authentication enable tacacs+**ã,³ãƒžãƒ³ãƒ‰ã�¯ã€�**enable**ã,³ãƒžãƒ³ãƒ‰ã�«å¯¾ã�—ã�¦TACACS+èª�è¨¼ã,'è¨å®šã�—ã�¾ **server host**ã,³ãƒžãƒ³ãƒ‰ã�¯ã€�TACACS+ã,µãƒ¼ãƒ�ã,'æŒ‡å®šã�—ã�¾ã�™ã€‚

Cisco Guardãƒ‡ãƒ�ã,¤ã,¹ã�¨Cisco Anomaly Traffic Detectorãƒ‡ãƒ�ã,¤ã,¹ã�Œå¤–éƒ¨TACACS+ã,µãƒ¼ãƒ�ã,'ä½¿ç”¨ã�—ã�¦ãƒ‡ãƒ�ã,¤ã,¹ã�«ãƒã,°ã,¤ãƒ **server host**ã,³ãƒžãƒ³ãƒ‰ã�§æŒ‡å®šã�•ã,Œã�¦ã�„ã�ªã�„å ´å�ˆã€�èª�è¨¼ã�¯ãƒ�ã,¤ãƒ'ã,¹ã�•ã,Œã�

- å˜åœ¨ã�—ã�ªã�„ã,¢ã,«ã,¦ãƒ³ãƒˆã�Œä½¿ç”¨ã�•ã,Œã�¦ã�„ã�¾ã�™ã€‚ãƒ¦ãƒ¼ã,¶ã�¯**show**ã

- ä½¿ç”¨ã�•ã,Œã�¦ã�„ã,‹æ—¢å˜ã�®ãƒãƒ¼ã,«ãƒ«ã,¢ã,«ã,¦ãƒ³ãƒˆï¼šãƒ¦ãƒ¼ã,¶ã�¯ã€�é€šå„ã�

- ä½¿ç”¨ã�•ã,Œã�¦ã�„ã,‹æ—¢å˜ã�®Linuxã,¢ã,«ã,¦ãƒ³ãƒˆï¼šãƒ¦ãƒ¼ã,¶ã�¯åŸºç›¤ã�¨ã�ªã,‹Lin

ã�¾ã�Ÿã€�TACACS+ã,µãƒ¼ãƒ�ã�«å¯¾ã�—ã�¦ã,¤ãƒ�ãƒ¼ãƒ–ãƒ«èª�è¨¼ã�Œ(**aaa authentication enable tacacs+**ã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç”¨ã�—ã�¦)å®Ÿè¡Œã�•ã,Œã€�å®Ÿéš›ã�®TACACS+ã,µãƒ¼ãƒ�ã�Œ(**taca server host**ã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç”¨ã�—ã�¦)æŒ‡å®šã�•ã,Œã�¦ã�„ã�ªã�„å ´å�ˆã�¯ã€�**enable**ã,³ãƒžãƒ³ãƒ

ãƒ‡ãƒ�ã,¤ã,¹ã�¯ã€�**tacacs-server host**ã,³ãƒžãƒ³ãƒ‰ã�ŒæŒ‡å®šã�•ã,Œã�¦ã�„ã�ªã�„å ´å�ˆã�«ã�®ã�¿è„†å¼±ã�§ã�,ã,‹ã�“ã�

ã�“ã�®è„†å¼±æ€§ã�¯ã€�Cisco Bug ID [CSCsd21455](ç™»éŒ²ãƒ¦ãƒ¼ã,¶å°,ç”¨)ã�«è¨˜è¼‰ã�•ã,Œã�¦ã�„ã�¾ã�™ã€,

å›žé�¿ç–

ã�“ã�®è„†å¼±æ€§ã�¯ã€�**tacacs-server host <IP address of TACACS+ server>**ã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç”¨ã�—ã�¦TACACS+ã,µãƒ¼ãƒ�ã,'æŒ‡å®šã�™ã,‹ã�“ã�¨ã�§ã€�TACAC

ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã�®ãƒ™ã,¹ãƒˆãƒ—ãƒ©ã,¯ãƒ†ã,£ã,¹ã�¨ã�—ã�¦ã€�ç®¡ç�†è€…ã�Œè¨å®šã�—ã� **wbm**ã,³ãƒžãƒ³ãƒ‰ã�¨**permit ssh**ã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç”¨ã�—ã�¾ã�™ã€,ã�“ã,Œã,‰ã�®ã,³ãƒžãƒ³ãƒ‰ã�«ã�¤ã�„ã�¦ã�¯ã€�ã

http://cisco.com/en/US/products/ps5888/products_configuration_guide_chapter09186a00804c0a6b.html#wp116244

ã�“ã,Œã,‰ã�®ã,¢ã,¯ã,»ã,¹å^¶å¾¡ãƒ¡ã,«ãƒ‹ã,ºãƒ ã,'å°Žå…¥ã�™ã,‹ã�¨ã€�ä¿¡é ¼ã�§ã��ã,‹ãƒ�ãƒ

ä¿®æ£æ¸ˆã�¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

ã�“ã�®è„†å¼±æ€§ã�¯ã€�Cisco Guardã�Šã,ˆã�³Cisco Traffic Anomaly Detectorã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®5.1ã,·ãƒªãƒ¼ã,ºã�§è§£æ±ºã�•ã,Œã�¦ã�„ã�¾ã�™ã€,5.1ã,·ãƒªãƒ¼

Cisco Guardã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ç”¨ã�®ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�¯ã€�http://www.cisco.com/pcgi-bin/tablebuild.pl/cisco-ga-cryptoã�‹ã,‰ãƒ€ã,¦ãƒ³ãƒãƒ¼ãƒ‰ã�§ã��ã�¾ã�™ã€,

Cisco Traffic Anomaly Detectorã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ç”¨ã�®ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�¯ã€�http://www.cisco.com/pcgi-bin/tablebuild.pl/cisco-ad-cryptoã�‹ã,‰ãƒ€ã,¦ãƒ³ãƒãƒ¼ãƒ‰ã�§ã��ã�¾ã�™ã€,

Cisco Catalyst 6500ã,¹ã,¤ãƒƒãƒ�/Cisco 7600ãƒ«ãƒ¼ã,¿ç”¨Cisco Anomaly

Guardãƒ¢ã‚¸ãƒ¥ãƒ¼ãƒ«ã�®ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã�¯ã€�http://www.cisco.com/pcgi-bin/tablebuild.pl/cisco-agm-cryptoã�‹ã‚‰ãƒ€ã‚¦ãƒ³ãƒãƒ¼ãƒ‰ã�§ã��ã�¾ã�™ã€‚

Cisco Catalyst 6500ã‚¹ã‚¤ãƒƒãƒ�/Cisco 7600ãƒ«ãƒ¼ã‚¿ç”¨Cisco Anomaly Traffic Detectorãƒ¢ã‚¸ãƒ¥ãƒ¼ãƒ«ã�®ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã�¯ã€�http://www.cisco.com/pcgi-bin/tablebuild.pl/cisco-adm-cryptoã�‹ã‚‰ãƒ€ã‚¦ãƒ³ãƒãƒ¼ãƒ‰ã�§ã��ã�¾ã�™ã€‚

ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã‚’æ¤œè¨Žã�™ã‚‹å ´å�ˆã�¯ã€�http://www.cisco.com/go/psirt
ã�¨å¾Œç¶šã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã‚‚å�‚ç…§ã�—ã�¦ã€�å•�é¡Œã�®è§£æ±ºçŠ¶æ³�ã�¨å®
ã‚½ãƒªãƒ¥ãƒ¼ã‚·ãƒ§ãƒ³ã‚’ç¢ºèª�ã�—ã�¦ã��ã� ã�•ã�„ã€‚

ã�„ã�šã‚Œã�®å ´å�ˆã‚‚ã€�ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã�™ã‚‹æ©Ÿå™¨ã�«å��åˆ†ã�ªãƒ¡ãƒ¢ãƒªã
Technical Assistance Centerï¼ˆTACï¼‰ã�¾ã�Ÿã�¯å¥‘ç´„ã‚’çµ�ã‚“ã�§ã�„ã‚‹ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã‚¹ãƒ—ãƒãƒ�ã‚¤ãƒ€ãƒ¼ã�«ã�Šå•�ã�„å�ˆã‚�ã�›ã��ã� ã�•ã�„ã€‚

ä¸�æ£åˆ©ç”¨äº‹ä¾‹ã�¨å…¬å¼�ç™ºè¡¨

Cisco PSIRT
ã�§ã�¯ã€�æœ¬ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�«è¨˜è¼‰ã�•ã‚Œã�¦ã�„ã‚‹è„†å¼±æ€§ã�®ä¸�æ£åˆ©ç

ã‚·ã‚¹ã‚³ã�¯ã€�ã�“ã�®å•�é¡Œã‚’å�–ã‚Šä¸Šã�’ã�ŸVerizon Businessã�®Gerrit Wenigæ°�ã�«æ„Ÿè¬�ã�„ã�Ÿã�—ã�¾ã�™ã€‚

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060215-guard

æ”¹è¨‚å±¥æ´

ãƒªãƒ“ã‚¸ãƒ§ãƒ³ 1.0	2006å¹´2æœˆ15æ—¥	åˆ�ç‰ˆãƒªãƒªãƒ¼ã‚¹

åˆ©ç”¨è¦�ç´„

æœ¬ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�¯ç„¡ä¿�è¨¼ã�®ã‚‚ã�®ã�¨ã�—ã�¦ã�”æ��ä¾›ã�—ã�¦ã�Šã‚Šã€
æœ¬ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�®æƒ…å ±ã�Šã‚ˆã�³ãƒªãƒ³ã‚¯ã�®ä½¿ç”¨ã�«é–¢ã�™ã‚‹è²¬ä»»ã�®ä¸€
ã�¾ã�Ÿã€�ã‚·ã‚¹ã‚³ã�¯æœ¬ãƒ‰ã‚ãƒ¥ãƒ¡ãƒ³ãƒˆã�®å†…å®¹ã‚’äºˆå‘Šã�ªã�—ã�«å¤‰æ›´ã�—ã
æœ¬ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�®è¨˜è¿°å†…å®¹ã�«é–¢ã�—ã�¦æƒ…å ±é…�ä¿¡ã�® URL
ã‚’çœ�ç•¥ã�—ã€�å�˜ç‹¬ã�®è»¢è¼‰ã‚„æ„�è¨³ã‚’æ–½ã�—ã�Ÿå ´å�ˆã€�å½“ç¤¾ã�Œç®¡ç

ã�“ã�®ãƒ‰ã‚ãƒ¥ãƒ¡ãƒ³ãƒˆã�®æƒ…å ±ã�¯ã€�ã‚·ã‚¹ã‚³è£½å“�ã�®ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ã‚’å¯¾è±¡ã