Cisco ASA 5500ã,·ãƒªãƒ¼ã,ºé€©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ Catalyst 6500ã,·ãƒªãƒ¼ã,ºASAã,µãƒ¼ãƒ“ã,¹ãƒ¢ã,¸ãƒ¥ãƒ¼ã

High

ã,¢ãƒ‰ãƒ¤ã,¶ãƒªãƒ¼ID : cisco-sa-20120314-asa

åˆ©å...¬é–‹æ—¥ : 2012-03-14 16:00

ãƒ¤ãƒ¼ã,¸ãƒ§ãƒ³ 1.0 : Final

CVSSã,¹ã,³ã,¢ : 7.8

å›žé¿ç– : No Workarounds available

Cisco ãƒ¤ã,° ID : CSCtq10441 CSCtu97367 CSCtw35765 CSCtr47517 CSCts39634

CVE-2012-0356 CVE-2012-0355 CVE-2012-0354 CVE-2012-0353

æ—¥æœ¬èªžã«ã,^ã,‹æƒ…å ±ã¯ã€è‹±èªžã«ã,^ã,‹åŽŸæ–‡ã®é€žå...¬å¼ã€

æ¦,è¦

Cisco ASA 5500ã,·ãƒªãƒ¼ã,ºé€©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹(ASA)ã€Šã,^ã€³Cisco Catalyst 6500ã,·ãƒªãƒ¼ã,ºASAã,µãƒ¼ãƒ“ã,¹ãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«(ASASM)ã¯ã€æ¬¡ã®è„†å¼±æ€§ã®å½±éŸ¿ã,

- Cisco ASA UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã®DoSè„†å¼±æ€§
- Cisco ASAã®è„...å¨¯æ¤œå‡ºã«ã€Šã‘ã‚‹DoSè„†å¼±æ€§
- Cisco ASA syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã®DoSè„†å¼±æ€§
- Protocol Independent Multicastã®Denial of Service(DoS)ã®è„†å¼±æ€§

ã“ã,Œã,‰ã®è„†å¼±æ€§ã¯ä°ã„ã«ç‹¬ç«‹ã—ã¦ã„ã¾ã™ã€‚ã„ã šã,Œã‹ã®è„

ã,·ã,¹ã,³ã¯ã“ã,Œã,‰ã®è„†å¼±æ€§ã«å¯¾å‡¦ã™ã‚‹ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã,'

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asa

**æ³¨ï¼šCisco Catalyst 6500ã,·ãƒªãƒ¼ã,ºFirewall Services Module(FWSM)ã¯ã€ä¸Šè¨˜ã®è„†å¼±æ€§ã®ä¸€éƒ¨ã®å½±éŸ¿ã,'å—ã'ã,‹å¯èƒ½æ€§ã

Cisco FWSMã€«å½±éŸ¿ã‚’å—ã‘ã¼ã€™è„†å¼±æ€§ã€«ã€¤ã€„ã€¦ã€¯ã€€å^¥é€”Cisco Security
Advisoryã€Œå…¬é–‹ã•ã‚Œã¦ã€„ã¾ã€™ã€‚ã“ã®ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã€¯ã€€https://sec.cisco.com/sa-20120314-fwsmã€§å…¥æ‰‹ã€§ã€€ã€¾ã€™ã€‚

è©²å½“è£½å“

Cisco ASA 5500ã‚·ãƒªãƒ¼ã‚ºé©©å¿œåž‹ã‚»ã‚ãƥãƪãƆã‚£ã‚¢ã‚¤ãƒã‚¹ã‚¢ãƒƒãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹ã¨Cisco Catalyst 6500ã‚·ãƪãƒ¼ã‚ºASAã‚µãƒ¼ãƒ“ã‚¹ã‚¢ãƥãƼãƫã€¯ã€€è¤‡æ•°ã€®è„†å¼±æ€§ã€®å½±éŸ¿ã‚’å—ã‘ASAã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ãƒªãƪãƼã‚¹ã€¯ã€€ç‰¹å®šã€®è„†å¼±æ€§ã€«ã‚ˆã€£ã€¦ç•°ã€

Cisco PIXã‚»ã‚ãƥãƪãƆã‚£ã‚¢ã‚¤ãƋã‚¹ã‚¢ãƳã‚¹ã€¯ã€€ã€“ã€®ã‚»ã‚¯ã‚·ãƧãƳã€«ã€¯ã€€PIXã€¯ãƒãƳãƆãƊãƳã‚¹ã€µãƒ¼ãƋã‚¹ã€Œçµä°†ã€—ã€¦ã€„ã€¾ã€™ã€‚Cisco PIXã‚»ã‚ãƥãƪãƆã‚£ã‚¢ã‚¤ãƋã‚¹ã‚¢ãƳã‚¹ã€¯ã€€ã€“ã€®ã€“ã€«ã€¯ã€€Cisco ASA 5500ã‚·ãƪãƒ¼ã‚ºé©©å¿œåž‹ã‚»ã‚ãƥãƪãƆã‚£ã‚¢ã‚¤ãƋã‚¹ã‚¢ãƳã‚¹ã€¸ã€®ç§»è¡Œã‚’ã€Šå‹§ã€PIXã‚»ã‚ãƥãƪãƆã‚£ã‚¢ã‚¤ãƋã‚¹ã‚¢ãƳã‚¹ã€¯ã€€å°†ç”¨ã‚¯ãƭãƳã‚¢ã€®ã€¿ã€§ã€™ã€‚

è„†å¼±æ€§ã€®ã€‚ã‚‹è£½å“

å…·ä½“çš„ã€ªãƒ‡ãƒã‚¤ã‚¹ãƳãƫæƒ…å ±ã€«ã€¤ã€„ã€¦ã€¯ã€€ã€“ã€®ã‚¢ãƉãƋã‚¤ã‚¶ãƪãƼã€«ã€¤ã€„ã€¦ã€¯ã€€ã€“ã€®ã€“ã€«ã€¯ã€€

Cisco ASA UDPã‚¤ãƳã‚¹ãƚã‚¯ã‚·ãƧãƳã‚¨ãƳã‚¸ãƳã€®DoSè„†å¼±æ€§

UDPãƒ™ãƼã‚¹ã€®ãƒ—ãƪãƈã‚³ãƫã€®æ¤œæŸ»ã€«ä½¿ç”¨ã€•ã‚Œã‚‹Cisco ASA UDPã‚¤ãƳã‚¹ãƚã‚¯ã‚·ãƧãƳã‚¨ãƳã‚¸ãƳã€¯ã€€è¤‡è¨¼ã€•ã‚Œã¦ã€„ã€ªã€„ã€„ãƪãƢãƼãƫã€®ã€¿ã€§ã€™ã€‚ã“ã€®è„†å¼±æ€§ã€Œå˜åœ¨ã€—ã€¦ã€„ã€¾ã€™ã€‚

Cisco ASA UDPã‚¤ãƳã‚¹ãƚã‚¯ã‚·ãƧãƳã‚¨ãƳã‚¸ãƳã€«ã€ˆã€£ã€¦æ¤œæŸ»ã€•ã‚Œã‚‹ã€‹ã€™ã€¹ã€¦ã€®UDPãƒ—ãƪãƈã‚³ãƫã€¯ã€€ASA UDPã‚¤ãƳã‚¹ãƚã‚¯ã‚·ãƧãƳã‚¨ãƳã‚¸ãƳã€‚ã€Œä½¿ç”¨ã€™ã‚‹ã€“ã€¨ã€ŒçŸ¥ã‚‰ã‚Œã€¦ã€„ã€¾ã€¹

- ãƒ‰ãƒ¡ã‚¤ãƳ ãƒ™ãƼã‚¹ ã‚·ã‚¹ãƆãƠï¼ˆDNSï¼‰
- Session Initiation Protocolï¼ˆSIPï¼‰
- Simple Network Management Protocolï¼ˆSNMPï¼‰
- GPRSãƈãƳãƒ«ãƪãƳã‚°ãƗãƈã‚³ãƫ(GTP)

- H.323ã€�H.225 RAS
- Media Gateway Control Protocolï¼ˆMGCPï¼‰
- sunrpc
- Trivial File Transfer Protocolï¼ˆTFTPï¼‰
- X Display Manager Control Protocol(XDMCP)
- IBM NetBios
- ã,¤ãƒ³ã,¹ã,¿ãƒ³ãƒˆãƒ¡ãƒƒã,»ãƒ¼ã,¸ï¼ˆä½¿ç”¨ã—ã�—ã�¦ã„ã,‹ç‰¹å®šã�®IMã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆ/ã

æ³¨ï¼šCisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�§ã�¯ã€�UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã�Œãƒ‡ãƒ•ã,©ãƒ«ãƒˆã�§

ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã�®æ¤œæŸ»æ¸ˆã�¿ãƒ•ãƒ¼ãƒˆã�¯ã€�æ¬¡ã�®ãƒªãƒ³ã,¯ã�«ãƒªã,¹ãƒˆã�•ã,Œã�
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/inspect_overview.html

æ³¨ï¼šCisco ASA UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã�¯ã€�class-mapã�Šã,ˆã�³policy-mapã,³ãƒžãƒ³ãƒ‰ã,’ä½¿ç”¨ã—ã�—ã¦ã€�ãƒ‡ãƒ•ã,©ãƒ«ãƒˆä»¥å¤–ã�®UDPãƒ•ãƒ¼ãƒˆã�«é�©ç”¨ã€
ASA
UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã,’ä½¿ç”¨ã™ã,‹ã,¤ãƒ³ã,¹ã,¿ãƒ³ã,¹ã«ã¯ã€�ã“ã®è„†å
ASA
UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã,’ä½¿ç”¨ã™ã,‹å ´å�ˆã�¯ã€�è„†å¼±æ€§ã�Œå˜åœ¨ã

ä¸Šè¨˜ã�®ã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã�®ã„ã�šã,Œã‹ã�Œæœ‰åŠ¹ã«ã�ªã£ã¦ã„ã,‹ã
show service-policy | include <inspection engine name>ã,³ãƒžãƒ³ãƒ‰ã,’ç™ºè¡Œã—ã€�ãƒžãƒƒãƒ‰ã�Œå‡ºåŠ›ã,’è¿”ã™ã“ã¨ã,’ç¢ºèª
NetBIOSãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ã,’æ¤œæŸ»ã™ã,‹ã,ˆã†ã«è¨å®šã•ã,Œã�ŸCisco ASAã,’ç¤ºã—ã¦ã„ã¾ã™ã€,

```
ciscoasa# show service-policy | include netbios
  Inspect: netbios, packet 0, drop 0, reset-drop 0
```

Cisco ASAã�®è„…å¨ï¿½æ¤œå‡ºã�«ã�Šã�'ã,‹DoSè„†å¼±æ€§

Cisco ASAã�®è„…å¨ï¿½æ¤œå‡ºæ©Ÿèƒ½ã�¯ã€�ã,¹ã,ãƒ£ãƒ³è„…å¨ï¿½ãƒ¢ãƒ¼ãƒ‰æ©Ÿèƒ½ã�¨*shun*ã,ªãƒ—
ASAã�®ãƒªãƒãƒ¼ãƒ‰ã,’å¼•ã��è¡·ã�“ã�™å¯¯èƒ½æ€§ã�®ã,ã‚‹è„†å¼±æ€§ã,’å«ã,“ã�§ã

Cisco ASA Threat Detection with Scanning Threatæ©Ÿèƒ½ï¿½
*shun*ã,ªãƒ—ã,·ãƒ§ãƒ³ã�Œæœ‰åŠ¹ã«ã�ªã£ã¦ã„ã‚‹ç¢ºèª�ã�™ã‚‹ã«ã�¯ã€**show running-config threat-detection scanning-threat**ã,³ãƒžãƒ³ãƒ‰ã,’ç™ºè¡Œã—ã€�ã‚Ÿå‡ºåŠ›ã«
*shun*ã,ªãƒ—ã,·ãƒ§ãƒ³ã�Œå«ã¾ã,Œã¦ã„ã‚‹ã“ã“ã¨ã,’ç¢ºèª�ã—ã¾ã™ã€,æ¬¡ã®ä¾‹ã

<#root>

```
ciscoasa# show running-config threat-detection scanning-threat
threat-detection scanning-threat
```

shun

æ³¨ï¼šã"ã®æ©Ÿèƒ½ã¯Cisco
ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³8.0(2)ã§å°Žå…¥ã•ã,Œã¾ã—ãŸ,Cis
ASAã®ä»¥å‰ã®ãƒãƒ¼ã,¸ãƒ§ãƒ³ã«ã¯ã¯ã,ã,Šã¾ã›ã,"ã€,

Cisco ASA syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã®DoSè„†å¼±æ€§

ã,µãƒ¼ãƒ“ã,¹æ‹’å¦(DoS)ã®è„†å¼±æ€§ã¯ã€ç‰¹å®šã•ã,·ã,¹ãƒ†ãƒ ãƒã,°(syslog)ãƒ¡ãƒƒã,»ãƒ¼
305006)ã®å®Ÿè£…ã«ã˜åœ¨ã—ã€»ãƒ¼ã,¸ã,'ç"Ÿæˆ•ã™ã,‹å¿…è¦
ASAã®ãƒªãƒãƒ¼ãƒ‰ã,'å¼•ã••èµ·ã"ã™å¯¾è±¡ã§ã,Šã¾ã™ã€,

Syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸ ID 305006ã¯ã€Cisco
ASAã,Œæ–°ã—ã„æŽ¥ç¶šã®ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã,¯ã,¢ãƒ‰ãƒ¬ã,¹å¤‰æ››(NAT)ã,'作æˆ•ã
ASA System Log Messagesã€•ã,¬ã,¤ãƒ‰ã,'å•,ç…§ã—ã—¦ã•ã• ã••ã„ã€,Cisco
ASAã§ã¯ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã§ã‚ãƒã,®ãƒ³ã,°ã¯æœ‰åŠ¹ã«ã•ªã£ã¦ã„ã¾ã›ã,"ã
ASAã¯è‡ªå‹•çš„ã«syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã,'æœ‰åŠ¹ã«ã—ã¾ã™ã€,

Cisco
ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã¯ã€æ¬¡ã®æ¡ä»¶ã•Œæº€ã•Ÿã••ã,Œã,‹ã¨ã€ã"ã®è„†å¼±æ

- ã,·ã,¹ãƒ†ãƒ ãƒã,®ãƒ³ã,°ã•Œæœ‰åŠ¹ã«ã•ªã£ã¦ã•Šã,Šã€•syslogã•Œä»»æ„•ã®
  syslogå®›å…ˆï¼ˆãƒ•ãƒƒãƒ•ã,¡ã„ASDMã•ªã•©ï¼‰ã«é€•ä¿¡ã••ã,Œã,‹ã,^ã•†ã•«è¨®šã
- Cisco
  ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•¯ã€•syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã,'ç"Ÿæˆ•ã•™ã,‹ã,^ã•†ã•«è¨®

Syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã•®ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã•®é‡•å¤§åº¦ãƒ¬ãƒ™ãƒ«ã•¯3ï¼ˆã,¨ãƒ©ãƒ¼ï¼
ï½ž 7ï¼‰ã•§ãƒ,®ãƒ³ã,°ã•Œè¨®šã••ã,Œã•¦ã•„ã,‹Cisco
ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•«ã•¯ã€•è„†å¼±æ€§ã•Œå˜åœ¨ã•™ã,‹å•¯èƒ½æ€§ã•Œã•,ã,Šã•¾ã

show
loggingã,³ãƒžãƒ³ãƒ‰ã,'ç™ºè¡Œã�—ã�¾ã�™ã€,æ¬¡ã�®ä¾‹ã�¯ã€�ãƒ¬ãƒ™ãƒ«6ï¼ˆæƒ…å ±ï¼‰ã€
ASAã,'ç¤ºã�—ã�¦ã„ã�¾ã�™ã€,

```
          ciscoasa# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level informational, 2 messages logged
    Trap logging: disabled
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã,'å�«ã,€ã,«ã,¹ã,¿ãƒ ãƒ¡ãƒƒã,»ãƒ¼ã,¸ãƒªã,¹ãƒˆ(**logging**
listã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç"¨ã�—ã�¦ä½œæˆ�ã�•ã,Œã�Ÿã,,ã�®)ã,'ã€�é‡�å¤§å°¦ã�¾ã�Ÿã�¯ãƒ

syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸ã�®ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã�®é‡�å¤§å°¦ãƒ¬ãƒ™ãƒ«ã�¯å¤‰æ›´ã�§ã��ã�¾ã€

**æ³¨ï¼šã�"ã�®è„†å¼±æ€§ã�¯ã€�æ–°ã�—ã„Cisco ASA Identity Firewall(IDFW)æ©Ÿèƒ½ã�®å®Ÿè£…å¾Œã�«å°Žå…¥ã�•ã,Œã�¾ã�—ã�Ÿã€,Cisco ASA IDFWæ©Ÿèƒ½ã�¯Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³8.4(2)ã�§å°Žå…¥ã�•ã,Œã�Ÿã,,ã€�Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ä»¥å‰�ã�®ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³ã�¯å½±éŸ¿ã,'å�—ã�'ã�¾ã�›ã,"ã€,

Protocol Independent Multicastã€®Denial of Service(DoS)ã€®è„†å¼±æ€§

Cisco
ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€¯ãƒžãƒ«ãƒ€ã,¹ãƒˆãƒ«ãƒ¼ãƒ†ã,£ãƒ³ã,°ã€Œæœ‰åŠ¹ãªå ´å€ˆã€
Indipendent
Multicast(PIM)ãƒ¡ãƒƒã,»ãƒ¼ã,¸ã€®å‡¦ç€†ä¸ã€«è©²å½“ãƒ‡ãƒ¤ã,¤ã,¹ã€®ãƒªãƒãƒ¼ãƒ‰ã,'å¼•ã€€

PIMã€Œã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã€§æœ‰åŠ¹ã€«ã€ªã€£ã€¦ã€„ã,‹ã€‹ã€©ã€†ã€‹ã,'ç¢ºèª€
pim
interfaceã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç”¨ã€—ã€¦ã€PIMåˆ—ã€®ä¸‹ã€«çŠ¶æ…‹*on*ã€Œè¡¨ç¤ºã€•ã,Œã,‹ã€

<#root>

```
          ciscoasa# show pim interface


Address          Interface          PIM  Nbr   Hello  DR         DR
                                         Count Intvl  Prior


192.168.1.1      outside
```

on

```
   0     30     1          this system

192.168.2.1      inside             off  0     30     1          this system
```

æ³¨ï¼šCisco ASAã€¯ã€€ show pim

interfaceã,³ãƒžãƒ³ãƒ‰å‡ºåŠ›ã�®PIMã,«ãƒ©ãƒ ã�®ä¸‹ã�«å°'ã�ªã��ã��¨ã,,1ã�¤ã�®ã,¤ãƒ³ã,¿ãƒ¼
*on*ã��ãƒžãƒ¼ã,¯ã�•ã,Œã�¦ã�„ã,‹å ´å^ˆã�«è„†å¼±ã�§ã�™ã€,

å®Ÿè¡Œã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ã�®å^¤å^¥

è„†å¼±æ€§ã�®ã�,ã,‹ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ã�® Cisco ASA
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�Œã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã�§å®Ÿè¡Œã•ã,Œã�¦ã�„ã,‹ã‹ã©ã†ã‹ã,'
show version
ã,³ãƒžãƒ³ãƒ‰ã,'ç™ºè¡Œã—ã¾ã™ã€,æ¬¡ã�®ä¾‹ã�¯ã€�ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ã
ASA
5500ã,·ãƒªãƒ¼ã,ºé�©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã,'ç¤ºã�—ã�¦ã�„ã¾ã™

```
ciscoasa#show version | include Version

Cisco Adaptive Security Appliance Software Version 8.4(1)

Device Manager Version 6.4(1)
```

Cisco Adaptive Security Device
Manager(ASDM)ã,'ä½¿ç"¨ã�—ã�¦ãƒ‡ãƒ�ã,¤ã,¹ã,'ç®¡ç�†ã�—ã�¦ã�„ã,‹ã�Šå®¢æ§˜ã�¯ã€�ãƒ
ASDMã,¦ã,£ãƒ³ãƒ‰ã,¦ã�®å·¦ä¸Šéš…ã�«è¡¨ç¤ºã�•ã,Œã,‹è¡¨ã�§ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒ�ãƒ¼ã,¸ãƒ§ã

Cisco
PIXã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã�«ã�¤ã�„ã�¦ã�®æƒ…å ±

Cisco
PIXã�¯ã€�ã�"ã�®ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�«è¨˜è¼‰ã�•ã,Œã�¦ã�„ã,‹ä¸€éƒ¨
PIXã�¯ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹ã,µãƒ�ãƒ¼ãƒˆã�Œçµ‚äº†ã�—ã�¦ã�„ã¾ã™ã€,Cisco
PIXã,'ã�"ä½¿ç"¨ã�®ã�Šå®¢æ§˜ã�«ã�¯ã€�Cisco
ASAã�¸ã�®ç§»è¡Œã,'ã�Šå‹§ã,�ã��ã�—ã¾ã™ã€,

Cisco

PIXã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ã™ã�¹ã�¦ã�®ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³ã
Independent Multicast Denial of Service Vulnerabilityã�®å½±éŸ¿ã,'å—ã�'ã¾ã™ã€,

Cisco
PIXã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³8.0ã�¯ã€�Cisco
ASA
UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã�®DoSè„†å¼±æ€§ã�®å½±éŸ¿ã,'å—ã�'ã¾ã™ã€,
Cisco ASAã�®è„…å¨ è¦¤æ¤œå‡ºã�«ã�Šã�'ã,‹DoSè„†å¼±æ€§

Cisco PIXã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã�¯ã€�Cisco ASA
syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã�®DoSè„†å¼±æ€§ã�®å½±éŸ¿ã,'å—ã�'ã¾ã›ã,"ã€,

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

Cisco
FWSMã,'é™¤ã��ã€�ä»–ã�®ã,·ã,¹ã,³è£½å"�ã�«ã�Šã�„ã�¦ã�"ã,Œã,‰ã�®è„†å¼±æ€§ã�®

è©³ç´°

æ¬¡ã�®ã,»ã,¯ã,·ãƒ§ãƒ³ã�§ã�¯ã€�å„è„†å¼±æ€§ã�«ã�¤ã�„ã�¦è©³ç´°ã�«èª¬æ˜Žã�—ã¾ã

Cisco ASA UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã�®DoSè„†å¼±æ€§

ã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ ã,¨ãƒ³ã,¸ãƒ³ã�¯ã€�ãƒ¦ãƒ¼ã,¶ã�®ãƒ‡ãƒ¼ã,¿ ãƒ'ã,±ãƒƒãƒˆå†…ã�« IP
ã,¢ãƒ‰ãƒ¬ãƒƒã,·ãƒ³ã,°æ…å ±ã,'åŸ‹ã,�è¾¼ã,€ã,µãƒ¼ãƒ"ã,¹ã,„ã€�ãƒ€ã,¤ãƒŠãƒŸãƒƒã,¯ã�«å‰²ã,Šå½"ã
ãƒ�ãƒ£ãƒ�ãƒ«ã,'é–‹ã��ã,µãƒ¼ãƒ"ã,¹ã�«å¿…è¦�ã�§ã�™ã€,Cisco
ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�¯ã€�UDPã�Šã,^ã�³TCPãƒ™ãƒ¼ã,¹ã�®ãƒ—ãƒãƒˆã,³ãƒ«ç"¨ã�«å¤šæ•°ã�®

UDPãƒ™ãƒ¼ã,¹ã�®ãƒ—ãƒãƒˆã,³ãƒ«ã�®æ¤œæŸ»ã�«ä½¿ç"¨ã�•ã,Œã,‹Cisco ASA
UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã�«ã�¯ã€�èª¤è¨¼ã�•ã,Œã�¦ã�„ã�ªã„ãƒªãƒ¢ãƒ¼ãƒˆã
ASAã�®ãƒªãƒãƒ¼ãƒ‰ã,'å¼•ã��èµ·ã�"ã�™å¯¯èƒ½æ€§ã�®ã,,ã,‹è„†å¼±æ€§ã�Œå˜åœ¨ã�—ã

ã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã�«ã,^ã�£ã�¦æ¤œæŸ»ã�•ã,Œã,‹ã�™ã�¹ã�¦ã�®UDPãƒ—ãƒãƒˆ

- ãƒ‰ãƒ¡ã,¤ãƒ³ ãƒ•ãƒ¼ãƒ ã,·ã,¹ãƒ†ãƒ ï¼ˆDNSï¼‰
- Session Initiation Protocolï¼ˆSIPï¼‰
- Simple Network Management Protocolï¼ˆSNMPï¼‰
- GPRSãƒˆãƒ³ãƒ•ãƒªãƒ³ã,°ãƒ—ãƒãƒˆã,³ãƒ«(GTP)
- H.323ã€�H.225 RAS
- Media Gateway Control Protocolï¼ˆMGCPï¼‰

- sunrpc
- Trivial File Transfer Protocolï¼ˆTFTPï¼‰
- X Display Manager Control Protocol(XDMCP)
- IBM NetBios
- ã,¤ãƒ³ã,¹ã,¿ãƒ³ãƒˆãƒ¡ãƒƒã,»ãƒ¼ã,¸ï¼ˆä½¿ç”¨ã—ã¦ã—ã¦ã„ã,‹ç‰¹å®šã®IMã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆ/ã,½

ã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã€Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€§ã€¯ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã€§æœ‰åŠ¹ã«ã€ªã£ã¦ã„ã,‹å ´å€ˆã€Œã€

**æ³¨ï¼šã€“ã€®è„†å¼±æ€§ã€®ä¸€æ£©ç”¨ã«ã¯ç”¨ã§ã,‹ã€®ã€¯ã€é€šé€šŽãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ IPv6 ãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ã€§ãƒˆãƒªã,¬ãƒ¼ã€•ã,Œã,‹å€¯èƒ½æ€§ã€Œã€,ã,Šã¾ã™ã€,ã€“ã€®è„†å¼±

ã€“ã€®è„†å¼±æ€§ã€¯ã€Cisco Bug ID CSCtq10441(ç™»éŒ²ãƒ¦ãƒ¼ã,¶å°,ç”¨)ã€¨ã€—ã€¦æ–‡æ›¸åŒ–ã•ã,Œã€Common Vulnerabilities and Exposures(CVE)IDã€¨ã€—ã€¦CVE-2012-0353ã€Œå‰²ã,Šå½“ã€¦ã,‰ã,Œã€¦ã€„ã¾ã™ã€,

Cisco ASAã€®è„…å¨ã€æ¤œå‡ºã€«ã€Šã€'ã,‹DoSè„†å¼±æ€§

Cisco ASAã€®è„…å¨ã€æ¤œå‡ºæ©Ÿèƒ½ã€¯ã€ã•ã¾ã–ã¾ãªè„…å¨ã«å¯¾ã—ã¦ã¦å€‹ã

Cisco ASA Threat Detectionæ©Ÿèƒ½ã,'Cisco ASAã,¹ã,ãƒ£ãƒ³è„…å¨ã‚¢ãƒ¼ã‚ãƒ‰æ©Ÿèƒ½ã€¨*shun*ã,ªãƒ—ã,·ãƒ§ãƒ³ã,'有åŠ¹ã«ã—ã¦ã„ã,‹å ´å€ˆã€ASAã€®ãƒªãƒãƒ¼ã‚¿ãƒ–ã€Œå¼•ã••ã,Œã,‹å€¯èƒ½æ€§ã€®ã,ã,‹è„†å¼±æ€§ã€Œç™ºç”

**æ³¨ï¼šã€“ã€®è„†å¼±æ€§ã€®ä¸€æ£©ç”¨ã«ã¯ç”¨ã§ã,‹ã€®ã€¯ã€é€šé€šŽãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ IPv6 ãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ã€§ãƒˆãƒªã,¬ãƒ¼ã€•ã,Œã,‹å€¯èƒ½æ€§ã€Œã€,ã,Šã¾ã™ã€,

ã€“ã€®è„†å¼±æ€§ã€¯ã€Cisco Bug ID CSCtw35765(ç™»éŒ²ãƒ¦ãƒ¼ã,¶å°,ç”¨)ã€¨ã€—ã€¦æ–‡æ›¸åŒ–ã•ã,Œã€CVE IDã€¨ã€—ã€¦CVE-2012-0354ã€Œå‰²ã,Šå½“ã€¦ã,‰ã,Œã€¦ã€„ã¾ã™ã€,

Cisco ASA syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã€®DoSè„†å¼±æ€§

Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€«ã€¯ã,·ã,¹ãƒ†ãƒ ãƒã,°(syslog)æ©Ÿèƒ½ã€Œã€,ã,Šã€é€šå„ã€®å‹•ä½œã€

ã,µãƒ¼ãƒ“ã,¹æ‹’å¦ã®è„†å¼±æ€§ã¯ã€1ã¤ã®ç‰¹å®šã®syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸(ãƒ¡ãƒƒã,»ãƒ¼ã,¸ID
305006)ã®å®Ÿè£…ã«å˜åœ¨ã—ã€ã“ã®syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸ã,'ç″Ÿæˆ•ã™ã,‹å¿…è¦•ã
ASAã®ãƒªãƒãƒ¼ãƒ‰ã,'å¼•ã••èµ·ã“ã™å¯¯èƒ½æ€§ã•Œã•,ã,Šã¾ã™ã€,æ″»æ'fè€…ã¯ã

Syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸ID 305006ã¯ã€Cisco
ASAã•Œæ–°ã—ã„æŽ¥ç¶šã®ãƒ•ãƒƒã‚¯ãƒ¼ãƒ‰ã,¯ã,¢ãƒ‰ãƒ¬ã,¹å¤‰æ•›(NAT)ã,'作æˆ•ã•§
ASAã,·ã,¹ãƒ†ãƒ ãƒã,°ãƒ¡ãƒƒã,»ãƒ¼ã,¸ã,¬ã,¤ãƒ‰ã€•ã,'å•,ç…§ã•—ã•¦ã••ã• ã••ã•„ã€,http://www.

**æ³¨ï¼šã•"ã•®è„†å¼±æ€§ã•®ä¸•æ£å^©ç"¨ã•«ä½¿ç"¨ã•§ã••ã,‹ã•®ã•¯ã€•é€šé•Žãƒˆãƒ©ãƒ
ãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ã•¨ IPv6
ãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ã•§ãƒˆãƒªã,¬ãƒ¼ã••ã,Œã,‹å•¯èƒ½æ€§ã•Œã•,ã,Šã¾ã™ã€,**

ã•"ã•®è„†å¼±æ€§ã•¯ã€•Cisco Bug ID CSCts39634(
ç™»éŒ²ãƒ¦ãƒ¼ã,¶å°,ç″¨)ã•¨ã•—ã•¦æ–‡æ›¸åŒ–ã••ã,Œã€•CVE IDã•¨ã•—ã•¦CVE-2012-
0355ã•Œå‰²ã,Šå½"ã•¦ã,‰ã,Œã•¦ã•„ã•¾ã•™ã€,

Protocol Independent Multicastã•®Denial of Service(DoS)ã•®è„†å¼±æ€§

ãƒžãƒ«ãƒ•ã,ãƒ£ã,¹ãƒˆãƒ«ãƒ¼ãƒ†ã,£ãƒ³ã,°ã•¯ã€•å•˜ä¸€ã•®æf…å ±ã,¹ãƒˆãƒªãƒ¼ãƒ ã,'è¤‡æ•°ã•®å•

Protocol Independent
Multicast(PIM)ã•¯ã€•IPãƒ«ãƒ¼ãƒ†ã,£ãƒ³ã,°ãƒ—ãƒãƒˆã,³ãƒ«ã•«ä¾•å˜ã•—ã•ªã•„ãƒžãƒ«ãƒ•ã,ãƒ£ã
Gateway Routing Protocol(EIGRP)ã€•Open Shortest Path First(OSPF)ã€•Border Gateway
Protocol(BGP)ã€•ã,¹ã,¿ãƒ†ã,£ãƒƒã,¯ãƒ«ãƒ¼ãƒˆã•ªã•©ã€•ä½¿ç"¨ä¸•ã•®ä»»æ„•ã•®ãƒ¦ãƒ‹ã,ãƒ£ã,¹

ãƒžãƒ«ãƒ•ã,ãƒ£ã,¹ãƒˆãƒ«ãƒ¼ãƒ†ã,£ãƒ³ã,°ã•Œæœ‰åŠ¹ã•«ã•ªã•£ã•¦ã•„ã,‹å ´å•^ã€•PIMãƒ¡ãƒƒ

**æ³¨ï¼šã•"ã•®è„†å¼±æ€§ã•¯ã€•ã,·ãƒ³ã,°ãƒ«ã,³ãƒ³ãƒ†ã,¹ãƒˆãƒ¢ãƒ¼ãƒ‰ã•®ãƒ«ãƒ¼ãƒ†ãƒƒãƒ‰ãƒ•
ASAã•«ã•®ã•¿å½±éŸ¿ã•—ã•¾ã•™ã€,PIM over
IPv6ã•¯ç•¾åœ¨ã,µãƒ•ãƒ¼ãƒˆã••ã,Œã•¦ã•„ã•ªã•„ã•Ÿã,•ã€•ã•"ã•®è„†å¼±æ€§ã•¯IPv4
PIMãƒ¡ãƒƒã,»ãƒ¼ã,¸ã•«ã,^ã•£ã•¦ã•®ã•¿å¼•ã••èµ·ã•"ã••ã,Œã•¾ã•™ã€,**

ã•"ã•®è„†å¼±æ€§ã•¯ã€•Cisco Bug ID CSCtr47517(
ç™»éŒ²ãƒ¦ãƒ¼ã,¶å°,ç″¨)ã•¨ã•—ã•¦æ–‡æ›¸åŒ–ã••ã,Œã€•CVE IDã•¨ã•—ã•¦CVE-2012-
0356ã•Œå‰²ã,Šå½"ã•¦ã,‰ã,Œã•¦ã•„ã•¾ã•™ã€,

å›žé¿ç–

æ¬¡ã•®ã,»ã,¯ã,·ãƒ§ãƒ³ã•§ã•¯ã€•ã•"ã•®ã,»ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƒªã•«è¨˜è¼‰ã••

Cisco ASA UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã�®DoSè„†å¼±æ€§

ã�“ã�®è„†å¼±æ€§ã,'è»½æ¸›ã�™ã,<å›žé�¿ç–ã�¯ã�,ã,Šã�¾ã�›ã,"ã€,

Cisco ASAã�®è„…å¨ �æ¤œå‡ºã�«ã�Šã'ã,<DoSè„†å¼±æ€§

*shun*ã,ªãƒ—ã,·ãƒ§ãƒ³,'有åŠ¹ã�«ã�™ã,<å¿…è¦ã�Œã�,ã,<å ´å�ˆã�¯ã€�ã“ã�®è„†å¼±æ€§ã,'è

ã“ã,Œã,'è¡Œã†ã«ã¯ã€�**no threat-detection scanning-threat shun**ã,³ãƒžãƒ³ãƒ‰ã,'ç™ºè¡Œã—ã¾ã™ã€,ã��ã•ã®å¾Œã€�**threat-detection scanning-threat**ã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç"¨ã™ã,<ã¨¨ã€�*shun*ã,ªãƒ—ã,·ãƒ§ãƒ³,'使ç"¨ã›ã•šã«ã“ã®æ©Ÿèƒ½

*shun*ã,ªãƒ—ã,·ãƒ§ãƒ³ã•Œæ£ã—ã••å‰Šé™¤ã••ã,Œã•Ÿã“ã¨ã,'ç¢ºèª•ã™ã,<ã«ã¯ã€�**sh running-config threat-detection scanning-threat**ã,³ãƒžãƒ³ãƒ‰ã,'ç™ºè¡Œã—ã¦ã€è¿"ã••ã,Œã•Ÿå‡ºåŠ›ã«*shun*ã,ªãƒ—ã,·ãƒ§ãƒ³ã•Œè¡¨ç¤ºã• *detection scanning-threat*æ©Ÿèƒ½ã,'è¨å®šã—ã•Ÿã“ã¨ã,'確èª•ã™ã,<ã•¨ã€•Cisco ASAã,'ç¤ºã—ã¦ã•„ã•¾ã•™ã€,

```
ciscoasa# show running-config threat-detection scanning-threat
threat-detection scanning-threat
```

Cisco ASA syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã�®DoSè„†å¼±æ€§

è€ƒã•ˆã,‰ã,Œã,‹å›žé�¿ç–ã•¯ã€•Cisco ASAã•Œç‰¹å®šã•®syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸ã,'ç"Ÿæˆ•ã••—ã•ªã•„ã,^ã•†ã•«ã•™ã,<ã•“ã•¨ã•§ã• **logging message 305006**ã,³ãƒžãƒ³ãƒ‰ã,'ç™ºè¡Œã—ã¾ã™ã€,

ãƒ¡ãƒƒã,»ãƒ¼ã,¸ã•Œç"Ÿæˆ•ã••ã,Œã•¦ã•„ã•ªã•„ã•“ã•¨ã,'ç¢ºèª•ã•™ã,<ã•«ã•¯ã€•**show running-configuration logging**ã,³ãƒžãƒ³ãƒ‰ã,'ç™ºè¡Œã—ã¾ã™ã€,æ¬¡ã•®ä¾‹ã•¯ã€•ãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã•®ãƒã,®

```
ciscoasa# show run logging
[...]
no logging message 305006
[...]
```

Protocol Independent Multicastã®Denial of Service(DoS)ã®è„†å¼±æ€§

PIMã,'æœ‰åŠ¹ã«ã™ã,‹å¿…è¦ã•ã,ã,‹å ´å•ˆã€•ã"ã®è„†å¼±æ€§ã,'è»½æ›ã™ã,‹å›žé

ãƒžãƒ«ãƒ•ã,ãƒ£ã,¹ãƒˆãƒ«ãƒ¼ãƒ†ã,£ãƒ³ã,°ã•Œå¿…è¦ã• ã•ŒPIMã•Œä½¿ç"¨ã••ã,Œã•¦ã•„ã•ª
no pimã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ãƒ¬ãƒ™ãƒ«ã,³ãƒžãƒ³ãƒ‰ã,'ç™ºè¡Œã•™ã,‹ã•"ã¨ã•§ã€•Cisco ASAã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã•§PIMã,'ç„¡åŠ¹ã•«ã•§ã••ã•¾ã•™ã€,

æ¬¡ã•®ä¾‹ã•¯ã€•PIMã•Œç„¡åŠ¹ã•«ã•ªã•£ã•¦ã•„ã,‹Cisco ASAãƒ‡ãƒ•ã,¤ã,¹ã•®ã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹Ethernet0/0ã,'ç¤ºã•—ã•¦ã•„ã•¾ã•™ã€,

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
 no pim
```

ã•™ã•¹ã•¦ã•®ã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã•§PIMã•Œç„¡åŠ¹ã•«ã•ªã•£ã•¦ã•„ã,‹ã•"ã¨ã,'ç¢ºè
pim
interfaceã,³ãƒžãƒ³ãƒ‰ã,'ç™ºè¡Œã•—ã€•ã•™ã•¹ã•¦ã•®ã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã•§PIMã•®çŠ¶æ
ASAã,'ç¤ºã•—ã•¦ã•„ã•¾ã•™ã€,

<#root>

```
ciscoasa# show pim interface

Address          Interface          PIM  Nbr   Hello  DR         DR
                                         Count Intvl  Prior

192.168.1.1      outside
off
  0     30     1          this system
192.168.2.1      inside
off
  0     30     1          this system
```

ä¿®æ£æ¸ˆã•¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,'æ¤œè¨Žã�™ã,‹å´å�ˆã�¯ã€�http://www.cisco.com/g
ã�® Cisco Security Advisories and Responses
ã,¢ãƒ¼ã,«ã,¤ãƒ–ã,„å¾Œç¶šã�®ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã,'å�,ç…§ã�—ã�¦ã€�ä¾µå®³ã,'å�—ã�'ã,‹å
ã,½ãƒªãƒ¥ãƒ¼ã,·ãƒ§ãƒ³ã,'ç¢ºèª�ã�—ã�¦ã��ã� ã�•ã„€,

ã�„ã�šã,Œã�®å´å�ˆã,,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,¹ãƒ—ãƒãƒ�ã,¤ãƒ€ãƒ¼ã

Cisco ASA UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã�®DoSè„†å¼±æ€§

è„†å¼±æ€§	ãƒ¡ã,¸ãƒ£ãƒ¼ãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼ˆä¿®æ£ã�•ã,Œã�Ÿæ
Cisco ASA UDPã,¤ãƒ³ã,¹ãƒšã,¯ã,·ãƒ§ãƒ³ã,¨ãƒ³ã,¸ãƒ³ã�®DoSè„†å¼±æ€§ â€“ CSCtq10441	7.0	Not affected
	7.1	Not affected
	7.2	Not affected
	8.0	8.0ï¼ˆ5.25ï¼‰
	8.1	8.1ï¼ˆ2.50ï¼‰
	8.2	8.2ï¼ˆ5.5ï¼‰
	8.3	8.3ï¼ˆ2.22ï¼‰
	8.4	8.4ï¼ˆ2.1ï¼‰
	8.5	8.5ï¼ˆ1.2ï¼‰
	8.6	Not affected

Cisco ASAã�®è„…å¨ï¿½æ¤œå‡ºã�«ã�Šã�'ã,‹DoSè„†å¼±æ€§

è„†å¼±æ€§	ãƒ¡ã,¸ãƒ£ãƒ¼ãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼ˆä¿®æ£ã�•ã,Œã�Ÿæœ€å^ï¿½ã�®ãƒªãƒªãƒ¼ã,¹ï¼‰
Cisco ASA Threat Detection Denial of Service Vulnerability - CSCtw35765	7.0	Not affected
	7.1	Not affected
	7.2	Not affected
	8.0	8.2(5.20)ã�¸ã�®ç§»è¡Œ
	8.1	8.2(5.20)ã�¸ã�®ç§»è¡Œ
	8.2	8.2ï¼ˆ5.20ï¼‰

	8.3	8.3ï¼^2.29ï¼‰
	8.4	8.4(3)
	8.5	8.5ï¼^1.6ï¼‰
	8.6	8.6ï¼^1.1ï¼‰

Cisco ASA syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã€®DoSè„†å¼±æ€§

è„†å¼±æ€§	ãƒ¡ã,¸ãƒ£ãƒ¼ãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼^ä¿®æ£ã€•ã,Œã€Ÿæœ€åˆ€ã
Cisco ASA syslogãƒ¡ãƒƒã,»ãƒ¼ã,¸305006ã€®DoSè„†å¼±æ€§ â€“ CSCts39634	7.0	Not affected
	7.1	Not affected
	7.2	Not affected
	8.0	Not affected
	8.1	Not affected
	8.2	Not affected
	8.3	Not affected
	8.41	8.4ï¼^2.11ï¼‰
	8.5	8.5ï¼^1.4ï¼‰
	8.6	Not affected

[1]ã€“ã€®è„†å¼±æ€§ã€¯ã€Identity Firewall(IDFW)ã€¨å'¼ã€°ã,Œã,‹æ–°ã€—ã€„Cisco ASAæ©Ÿèƒ½ã€®å®Ÿè£…å¾Œã€«åº'å…¥ã€•ã,Œã€¾ã€—ã€Ÿã€,Cisco ASA IDFWæ©Ÿèƒ½ã€¯Cisco ASAãƒ€ãƒ¼ã,¸ãƒ§ãƒ³8.4(2)ã€§å°'å…¥ã€•ã,Œã€Ÿã€Ÿã,€ã€Cisco ASAã€®ä»¥å‰‍ã€®ãƒ€ãƒ¼ã,¸ãƒ§ãƒ³ã€¯å½±éŸ¿ã,'å€—ã€'ã€¾ã€›ã,"ã€,

Protocol Independent Multicastã€®Denial of Service(DoS)ã€®è„†å¼±æ€§

è„†å¼±æ€§	ãƒ¡ã,¸ãƒ£ãƒ¼ãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼^ä¿®æ£ã€•ã,Œã€Ÿæœ€åˆ€ã€®ãƒªãƒªãƒ¼
Protocol Independent Multicast(PIM)ã€®DoSè„†å¼±æ€§ â€“ CSCtr47517	7.0	7.2(5.7)ã€¸ã€®ç§»è¡Œ
	7.1	7.2(5.7)ã€¸ã€®ç§»è¡Œ
	7.2	7.2ï¼^5.7ï¼‰
	8.0	8.0ï¼^5.27ï¼‰
	8.1	8.1ï¼^2.53ï¼‰

	8.2	8.2ï¼ˆ5.8ï¼‰
	8.3	8.3ï¼ˆ2.25ï¼‰
	8.4	8.4ï¼ˆ2.5ï¼‰
	8.5	8.5ï¼ˆ1.2ï¼‰
	8.6	Not affected

æŽ¨å¥¨ãƒªãƒªãƒ¼ã‚¹

æ¬¡ã�®è¡¨ã«ã€€ã€€ã€€ã€™ã€¹ã€¦ã€®æŽ¨å¥¨ãƒªãƒªãƒ¼ã‚¹ã‚’ç¤ºã—ã—ã¾ã™ã€‚ã“ã‚Œã‚‰ã®

ãƒ¡ã‚¸ãƒ£ãƒ¼ ãƒªãƒªãƒ¼ã‚¹	æŽ¨å¥¨ãƒªãƒªãƒ¼ã‚¹
7.0	7.2(5.7)ã€‚ã€®ç§»è¡Œ
7.1	7.2(5.7)ã€‚ã€®ç§»è¡Œ
7.2	7.2ï¼ˆ5.7ï¼‰
8.0	8.2(5.26)ã€‚ã€®ç§»è¡Œã€Œå¿…è¦
8.1	8.2(5.26)ã€‚ã€®ç§»è¡Œã€Œå¿…è¦
8.2	8.2ï¼ˆ5.26ï¼‰
8.3	8.4ï¼ˆ3.8ï¼‰
8.4	8.4ï¼ˆ3.8ï¼‰
8.5	8.5ï¼ˆ1.7ï¼‰
8.6	8.6ï¼ˆ1.1ï¼‰

ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã€®ãƀã‚¦ãƳãƼãƉ

Cisco ASAã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ã€¯ã€€Software Center(Cisco.com)ã€‹ã‚‰ãƀã‚¦ãƳãƼãƉã€§ã€€ã€¾ã€™ã€‚
http://www.cisco.com/cisco/software/navigator.html

Cisco ASA 5500ã‚·ãƪãƼã‚ºé©©å¿œåž‹ã‚»ã‚ãƥãƪãƆã‚£ã‚¢ãƗãƳã‚¹ã‚¢ã€¯ã€€ã€[è£½å“](Pro > [ã‚»ã‚ãƥãƪãƆã‚£(Security)] > [ãƒ•ã‚¡ã‚¤ã‚¢ã‚¦ã‚©ãƼãƫ(Firewall)] > [ãƒ•ã‚¡ã‚¤ã‚¢ã‚¦ã‚©ãƼãƫã‚¢ãƗãƳã‚¹ã‚¢ã€¹(Firewall Appliances)] > [Cisco ASA

5500ã,·ãƒªãƒ¼ã,ºé•©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹(Cisco ASA Series Adaptive Security Appliances)] > <Cisco ASAãƒ¢ãƒ‡ãƒ«> > [é•©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹(ASA)ã,½ãƒ•ãƒˆã,¦ã,§ã,¢(Adaptive Security Appliance (ASA Software)]
ã•«ç§»å‹•ã•—ã•¾ã•™ã€‚ã•“ã,Œã,‰ã•®ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³ã•®ä¸€éƒ¨ã•¯æš«å®šãƒ•ãƒ¼ã,¸ãƒ§ã
ã,¿ãƒ–ã,’å±•é–‹ã•™ã,‹ã•¨è¡¨ç¤ºã••ã,Œã•¾ã•™ã€,

Cisco Catalyst 6500ã,·ãƒªãƒ¼ã,ºASAã,µãƒ¼ãƒ“ã,¹ãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«ã•®å ´å•ˆã•¯ã€•[è£½å“•(Products)] > [Ciscoã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã•Šã,ˆã•³ãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«(Cisco Interfaces and Modules)] > [Ciscoã,µãƒ¼ãƒ“ã,¹ãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«(Cisco Services Modules)] > [Cisco Catalyst 6500ã,·ãƒªãƒ¼ã,ºASAã,µãƒ¼ãƒ“ã,¹ãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«(Cisco Catalyst 6500 Series ASA Services Module)] > [ASAã,µãƒ¼ãƒ“ã,¹ãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«(ASASM)ã,½ãƒ•ãƒˆã,¦ã,§ã,¢(ASA Services Module (ASASM Software)]
ã•«ç§»å‹•ã•—ã•¾ã•™ã€‚ã•“ã,Œã,‰ã•®ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³ã•®ä¸€éƒ¨ã•¯æš«å®šãƒ•ãƒ¼ã,¸ãƒ§ã
ã,¿ãƒ–ã,’å±•é–‹ã•™ã,‹ã•¨è¡¨ç¤ºã••ã,Œã•¾ã•™ã€,

ä¸€æ£åˆ©ç”¨äº‹ä¾‹ã•¨å…¬å¼€ç™ºè¡¨

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

ã•“ã•®ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã•«è¨˜è¼‰ã••ã,Œã•¦ã•„ã,‹ã•™ã•¹ã•¦ã•®è„

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asa

æ”¹è¨‚å±¥æ´

ãƒªãƒ“ã,¸ãƒ§ãƒ³ 1.0	2012å¹´3月14æ—¥	åˆ•ç‰ˆãƒªãƒªãƒ¼ã,¹

åˆ©ç”¨è¦•ç´„

本アドバイザリの情報は、本ドキュメントに記載されている製品を使用されるお客様を対象に提供されています。シスコでは、本アドバイザリの情報の正確性を確認するために合理的な努力を払っていますが、お客様による本アドバイザリの情報の評価はお客様の責任で行っていただくものとします。シスコは、本アドバイザリの情報が不正確であったり、本アドバイザリの情報に従わなかったりしたことに起因する一切の損害に対して責任を負いません。本アドバイザリの情報は、予告なく変更、更新、または廃止されることがあります。本アドバイザリの 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,¹ã,³è£½å“•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。