Cisco Firepower Threat Defense ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�® DNS é�©ç”¨ã�«ã�Šã�‘ã,‹ã,µãƒ¼ãƒ“ã,¹å¦¨å®³ã�

High

ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªãƒ¼ID : cisco-sa-FTD-snort3-DOS-Aq38LVdM

åˆ�å…¬é–‹æ—¥ : 2022-04-27 16:00

ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ 1.0 : Final

CVSSã,¹ã,³ã,¢ : 8.6

å›žé�¿ç– : No workarounds available

Cisco ãƒ�ã,° ID : CSCwa21016

CVE-2022-20767

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

æ¦‚è¦�

Cisco Firepower Threat Defenseï¼ˆFTDï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�® Snort ãƒ«ãƒ¼ãƒ«è©•ä¾¡æ©Ÿèƒ½ã�«ã�Šã�‘ã,‹è„†å¼±æ€§ã�«ã,ˆã,Šã€�èª�è¨¼ã�•ã,Œã�¦ã�„ã�ªã�„

ã�“ã�®è„†å¼±æ€§ã�¯ã€�DNS ãƒ¬ãƒ"ãƒ¥ãƒ†ãƒ¼ã,·ãƒ§ãƒ³é�©ç”¨ãƒ«ãƒ¼ãƒ«ã�®ä¸�é�©åˆ‡ã�ªå‡¦ç�†ã�«èµ·å› ã�—ã�¾ã�™ã€ UDP ãƒ'ã,±ãƒƒãƒˆã,'é€�ä¿¡ã�™ã,‹ã�"ã�¨ã�«ã,ˆã,Šã€�ã�"ã�®è„†å¼±æ€§ã,'ã,¨ã,¯ã,¹ãƒ—ãƒã,¤ãƒˆã�™ DoS çŠ¶æ…‹ã�Œç™ºç"Ÿã�™ã,‹å�¯èƒ½æ€§ã�Œã�,ã,Šã�¾ã�™ã€,

æ³¨ï¼šã�"ã�®è„†å¼±æ€§ã�¯ã€�Snort 3ã,'å®Ÿè¡Œã�—ã�¦ã�„ã,‹Cisco FTDãƒ‡ãƒ�ã,¤ã,¹ã�«ã�®ã�¿å½±éŸ¿ã,'ä¸Žã�ˆã�¾ã�™ã€,

ã,·ã,¹ã,³ã�¯ã�"ã�®è„†å¼±æ€§ã�«å¯¾å‡¦ã�™ã,‹ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã,'ãƒªãƒªãƒ¼

ã�"ã�®ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�¯ã€�æ¬¡ã�®ãƒªãƒ³ã,¯ã,ˆã,Šç¢ºèª�ã�§ã��ã�¾ã�™ã€, https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FTD-snort3-DOS-Aq38LVdM

ã�"ã�®ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�¯ã€�2022 å¹´ 4 æœˆã�«å…¬é–‹ã�•ã,Œã�Ÿ Cisco ASAã€�FTDã€�ã�Šã,ˆã�³ FMC ã�®ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒª ãƒ�ãƒ³ãƒ‰ãƒ«ã�«å�«ã�¾ã,Œã�¦ã�„ã�¾ã�™ã€,ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�¨ãƒªãƒ³ã,¯ã�®ä¸€è¦§ Event Responseï¼š2022 å¹´ 4 æœˆã�«å…¬é–‹ã�•ã,Œã�Ÿ Cisco ASAã€�FMCã€�ã�Šã,ˆã�³ FTD

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒª ãƒ�ãƒ³ãƒ‰ãƒ«
ã,'å�,ç…§ã�—ã�¦ã���ã� ã�•ã�„ã€,

è©²å½"è£½å"�

è„†å¼±æ€§ã�®ã�,ã,‹è£½å"�

ã�"ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã,'å�—ã�'ã,‹ã�®ã�¯ã€�ã,·ã,¹ã,³ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ ã�
Cisco FTD
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã�Œå®Ÿè¡Œã�•ã,Œã€�æ¬¡ã�®ä¸¡æ–¹ã�®æ�¡ä»¶ã,'æº€ã�Ÿã�

- ãƒ‡ãƒ�ã,¤ã,¹ã�§ Snort 3 ã,'å®Ÿè¡Œã�—ã�¦ã�„ã,‹ã€,
- ãƒ‡ãƒ�ã,¤ã,¹ã�§ DNS ãƒ¬ãƒ"ãƒ¥ãƒ†ãƒ¼ã,·ãƒ§ãƒ³é�©ç"¨ã�Œæœ‰åŠ¹ã�«ã�ªã�£ã�¦ã�„ã,‹ã€,

è„†å¼±æ€§ã�Œå˜åœ¨ã�™ã,‹ Cisco
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã�«ã�¤ã�„ã�¦ã�¯ã€�ã�"ã�®ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�®ã€Œä

Snort 3 ã�¯ã€�Cisco FTD ãƒªãƒªãƒ¼ã,¹ 7.0.0
ä»¥é™�ã�®æ–°è¦�ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ã�®å ´å�ˆã€�ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã�§å®Ÿè¡Œã�•ã,Œã�¦
FTD ãƒªãƒªãƒ¼ã,¹ 6.7.0 ä»¥å‰�ã,'å®Ÿè¡Œã�—ã�¦ã�„ã�¦ã€�ãƒªãƒªãƒ¼ã,¹ 7.0.0
ä»¥é™�ã�«ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã�•ã,Œã�Ÿãƒ‡ãƒ�ã,¤ã,¹ã�§ã�¯ã€�Snort 2
ã�Œãƒ‡ãƒ•ã,©ãƒ«ãƒˆã�§å®Ÿè¡Œã�•ã,Œã�¦ã�„ã�¾ã�™ã€,

DNS ãƒ¬ãƒ"ãƒ¥ãƒ†ãƒ¼ã,·ãƒ§ãƒ³é�©ç"¨ã�¯ã€�Cisco FTD ãƒªãƒªãƒ¼ã,¹ 6.7
ä»¥é™�ã�§ã�¯ãƒ‡ãƒ•ã,©ãƒ«ãƒˆã�§æœ‰åŠ¹ã�«ã�ªã�£ã�¦ã�„ã�¾ã�™ã€,DNS
ãƒ¬ãƒ"ãƒ¥ãƒ†ãƒ¼ã,·ãƒ§ãƒ³é�©ç"¨ã�¯ã€�Cisco FTD ãƒªãƒªãƒ¼ã,¹ 6.7
ã�§å°Žå…¥ã�•ã,Œã�¾ã�—ã�Ÿã€,

FTD CLI ã�«ã,ˆã,‹ Cisco FTD è¨å®šã�®ç¢ºèª�

Snort 3
ã�Œãƒ‡ãƒ�ã,¤ã,¹ã�§è¨å®šã�•ã,Œã�¦ã�„ã,‹ã�‹ã�©ã�†ã�‹ã,'ç¢ºèª�ã�™ã,‹ã�«ã�¯ã€�FT
CLI ã�«ãƒã,°ã,¤ãƒ³ã�—ã€�**show snort3 status**
ã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç"¨ã�—ã�¾ã�™ã€,ã,³ãƒžãƒ³ãƒ‰ã�«ã,ˆã�£ã�¦æ¬¡ã�®å‡ºåŠ›ã�Œç"Ÿæˆ�ã
Snort 3
ã,'å®Ÿè¡Œã�—ã�¦ã�„ã�¦ã€�ã�"ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã,'å�—ã�'ã,‹å�¯èƒ½æ€§ã�Œ

```
<#root>

>

show snort3 status
```

```
Currently running Snort 3
```

DNS ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã,·ãƒ§ãƒ³é�©ç”¨ã�Œæœ‰åŠ¹ã�«ã�ªã�£ã�¦ã�„ã,‹ã�‹ã�©ã�†ã�‹ã,’ç¢ºèª�

1. FTD CLI ã�«ãƒã,°ã,¤ãƒ³ã�—ã�¾ã�™ã€,
2. **expert** ã,³ãƒžãƒ³ãƒ‰ã,’ä½¿ç”¨ã�—ã�¦ã,¨ã,ã,¹ãƒ'ãƒ¼ãƒˆãƒ¢ãƒ¼ãƒ‰ã�«ã�—ã�¾ã�™ã€,
3. luaãƒ‡ã,£ãƒ¬ã,¯ãƒˆãƒªã�«ç§»å‹•ã�—ã�¾ã�™ã€, ã�"ã�®ãƒ‡ã,£ãƒ¬ã,¯ãƒˆãƒªã�¯ã€�/ngfw/v FTDã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ã�®ãƒ¦ãƒ‹ãƒ�ãƒ¼ã,µãƒ«ä¸€æ„�è˜åˆ¥å�ã�§ã�™ã€,
4. **grep** ã,³ãƒžãƒ³ãƒ‰ã,'ä½¿ç"¨ã�—ã�¦ã€�lua ãƒ‡ã,£ãƒ¬ã,¯ãƒˆãƒªã�® *firewall.lua* ãƒ•ã,¡ã,¤ãƒ«ã�§ *dns_filter* ã,'æ¤œç´¢ã�—ã�¾ã�™ã€,
   - ãƒ•ã,¡ã,¤ãƒ«ã�« **dns_filtering_enabled = true** ã�Œå�«ã�¾ã,Œã�¦ã�„ã,‹å ´å�ˆã€�ãƒ‡ãƒ�ã,¤ã,¹ã�¯ã�"ã�®è„†å¼±æ€§ã�®å½
   - ãƒ•ã,¡ã,¤ãƒ«ã�« **dns_filtering_enabled = false** ã�Œå�«ã�¾ã,Œã�¦ã�„ã,‹å ´å�ˆã€�ãƒ‡ãƒ�ã,¤ã,¹ã�¯ã�"ã�®è„†å¼±æ€§ã�®å½
   - **dns_filtering_enabled** ã�Œãƒ•ã,¡ã,¤ãƒ«ã�«å�«ã�¾ã,Œã�¦ã�„ã�ªã�„å ´å�ˆã€�ãƒ‡ãƒ�ã,¤ã,¹ã�¯ã�"ã�

```
>expert
expert admin@ftd700:~$ cd /ngfw/var/sf/detection_engines/e4dec56e-ef9e-11eb-b690-6843d4a521ed/lua/
expert admin@ftd700:~$ grep dns_filter firewall.lua
 dns_filtering_enabled = true
```

æ³¨ï¼šshow **access-control-config**ã,³ãƒžãƒ³ãƒ‰ã�§ã�¯ã€�ä¸�å…·å�ˆCSCwb37077ã�ŒåŽŸå› ã�§ã€�DNSãƒ¬ãƒ"ãƒ¥ãƒ†ãƒ¼ã,

Cisco Firepower Management Centerï¼ˆFMCï¼‰ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã,¤ã,¹ã�® Cisco FTD è¨å®šã�®ç¢ºèª�

Snort 3 ã�Œãƒ‡ãƒ�ã,¤ã,¹ã�§è¨å®šã�•ã,Œã�¦ã�„ã,‹ã�‹ã�©ã�†ã�‹ã,'ç¢ºèª�ã�™ã,‹ã�«ã�¯ã€�æ

1. FMC Web ã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã�«ãƒã,°ã,¤ãƒ³ã�—ã�¾ã�™ã€,
2. [ãƒ‡ãƒ�ã,¤ã,¹ï¼ˆDevicesï¼‰] ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã,‰ [ãƒ‡ãƒ�ã,¤ã,¹ç®¡ç�†ï¼ˆDevice Managementï¼‰] ã,'é�¸æŠžã�—ã�¾ã�™ã€,
3. é�©åˆ‡ã�ª FTD ãƒ‡ãƒ�ã,¤ã,¹ã,'é�¸æŠžã�—ã�¾ã�™ã€,
4. [ç·¨é›†ï¼ˆEditï¼‰]

ã‚¢ã‚¤ã‚³ãƒ³ï¼ˆé‰›ç†ã�®å½¢ï¼‰ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚

5. [ãƒ‡ãƒ�ã‚¤ã‚¹ï¼ˆDeviceï¼‰] ã‚¿ãƒ–ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã€�[æ¤œæŸ»ã‚¨ãƒ³ã‚¸ãƒ³ï¼ˆInspection Engineï¼‰] é ˜åŸŸã‚’ç¢ºèª�ã�—ã�¾ã�™ã€‚
   - ã€Œ**Snort 2**ã€�ã�Œç¤ºã�•ã‚Œã�¦ã�„ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�¯ã�“ã�®è„†å¼±æ€§ã�®
   - ã€Œ**Snort 3**ã€�ã�Œç¤ºã�•ã‚Œã�¦ã�„ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�¯ã�“ã�®è„†å¼±æ€§ã�®

DNS ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã�Œæœ‰åŠ¹ã�«ã�ªã�£ã�¦ã�„ã‚‹ã�‹ã�©ã�†ã�‹ã‚’ç¢ºèª�

1. FMC Web ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ãƒã‚°ã‚¤ãƒ³ã�—ã�¾ã�™ã€‚
2. [ãƒ�ãƒªã‚·ãƒ¼ï¼ˆPoliciesï¼‰] ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã‚‰ [ã‚¢ã‚¯ã‚»ã‚¹åˆ¶å¾¡ï¼ˆAccess Controlï¼‰] ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚
3. ç¢ºèª�ã�™ã‚‹ãƒ�ãƒªã‚·ãƒ¼ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚
4. [ç·¨é›†ï¼ˆEditï¼‰] ã‚¢ã‚¤ã‚³ãƒ³ï¼ˆé‰›ç†ã�®å½¢ï¼‰ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
5. [Advanced] ã‚¿ãƒ–ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
6. [å…¨èˆ¬è¨å®šï¼ˆGeneral Settingsï¼‰] é ˜åŸŸã�§ã€�[DNSãƒˆãƒ©ãƒ•ã‚£ãƒƒã‚¯ã�¸ã�®ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã‚’æœ‰åŠ¹ reputation enforcement on DNS trafficï¼‰] ã‚’ç¢ºèª�ã�—ã�¾ã�™ã€‚
   - è¨å®šã�Œã€Œ**Yes**ã€�ã�§ã�‚ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�¯ã�“ã�®è„†å¼±æ€§ã�®
   - è¨å®šã�Œã€Œ**No**ã€�ã�§ã�‚ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�¯ã�“ã�®è„†å¼±æ€§ã�®

Cisco Firepower Device Managementï¼ˆFDMï¼‰ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã‚¤ã‚¹ã�® Cisco FTD è¨å®šã�®ç¢ºèª�

Snort 3 ã�Œãƒ‡ãƒ�ã‚¤ã‚¹ã�§è¨å®šã�•ã‚Œã�¦ã�„ã‚‹ã�‹ã�©ã�†ã�‹ã‚’ç¢ºèª�ã�™ã‚‹ã�«ã�¯ã€�æ

1. FTD Web ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ãƒã‚°ã‚¤ãƒ³ã�—ã�¾ã�™ã€‚
2. ãƒ¡ã‚¤ãƒ³ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã‚‰ [ãƒ�ãƒªã‚·ãƒ¼ï¼ˆPoliciesï¼‰] ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚
3. [ä¾µå…¥ï¼ˆIntrusionï¼‰] ã‚¿ãƒ–ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
4. [æ¤œæŸ»ã‚¨ãƒ³ã‚¸ãƒ³ï¼ˆInspection Engineï¼‰] ã�§æ¤œæŸ»ã‚¨ãƒ³ã‚¸ãƒ³ã�®ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã‚’ç¢ºèª�ã�—ã�¾ã�™ã€‚ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã� 2 ã�®å ´å�ˆã�¯ã€Œ*2*ã€�ã�§å§‹ã�¾ã‚Šã€�Snort 3 ã�®å ´å�ˆã�¯ã€Œ*3ã€�ã�§å§‹ã�¾ã‚Šã�¾ã�™ã€‚*
   - ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã�Œã€Œ*2*ã€�ã�§å§‹ã�¾ã�£ã�¦ã�„ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�

Snort 2
ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã‚’å®Ÿè¡Œã�—ã�¦ã�Šã‚Šã€�ã�“ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã‚’å�

- ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã�Œã€Œ3ã€�ã�§å§‹ã�¾ã�£ã�¦ã�„ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�
  Snort 3
  ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã‚’å®Ÿè¡Œã�—ã�¦ã�Šã‚Šã€�ã�“ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã‚’å�

DNS

ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã�Œæœ‰åŠ¹ã�«ã�ªã�£ã�¦ã�„ã‚‹ã�‹ã�©ã�†ã�‹ã‚’ç¢ºèª�

1. FTD Web ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ãƒã‚°ã‚¤ãƒ³ã�—ã�¾ã�™ã€‚
2. ãƒ¡ã‚¤ãƒ³ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã‚‰ [ãƒ�ãƒªã‚·ãƒ¼ï¼ˆPoliciesï¼‰] ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚
3. [ã‚¢ã‚¯ã‚»ã‚¹åˆ¶å¾¡ï¼ˆAccess Controlï¼‰]ã‚¿ãƒ–ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
4. [è¨å®šï¼ˆSettingsï¼‰] ã‚¢ã‚¤ã‚³ãƒ³ï¼ˆæ¯è»Šã�®å½¢ï¼‰ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
5. [DNSãƒˆãƒ©ãƒ•ã‚£ãƒƒã‚¯ã�¸ã�®ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ï¼ˆReputation Enforcement on DNS trafficï¼‰] ã‚’ç¢ºèª�ã�—ã�¾ã�™ã€‚
   - è¨å®šã�Œã‚ªãƒ³ã�§ã�‚ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�¯ã�“ã�®è„†å¼±æ€§ã�®å½±éŸ
   - è¨å®šã�Œã‚ªãƒ•ã�§ã�‚ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�¯ã�“ã�®è„†å¼±æ€§ã�®å½±éŸ

Cisco Defense Orchestrator ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã‚¤ã‚¹ã�® Cisco FTD è¨å®šã�®ç¢ºèª�

Snort 3

ã�Œè¨å®šã�•ã‚Œã�¦ã�„ã‚‹ã�‹ã�©ã�†ã�‹ã‚’ç¢ºèª�ã�™ã‚‹ã�«ã�¯ã€�æ¬¡ã�®æ‰‹é †ã‚’

1. Cisco Defense Orchestrator Web ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ãƒã‚°ã‚¤ãƒ³ã�—ã�¾ã�™ã€‚
2. [ã‚¤ãƒ³ãƒ™ãƒ³ãƒˆãƒªï¼ˆInventoryï¼‰] ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã‚‰ é�©åˆ‡ã�ª FTD ãƒ‡ãƒ�ã‚¤ã‚¹ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚
3. [ãƒ‡ãƒ�ã‚¤ã‚¹ã�®è©³ç´°ï¼ˆDevice Detailsï¼‰] é ˜åŸŸã�§ã€�[Snortãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ï¼ˆSnort Versionï¼‰] ã‚’ç¢ºèª�ã�—ã�¾ã�™ã€‚ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã�¯ã€�Snort 2 ã�®å ´å�ˆã�¯ã€Œ2ã€�ã�§å§‹ã�¾ã‚Šã€�Snort 3 ã�®å ´å�ˆã�¯ã€Œ3ã€�ã�§å§‹ã�¾ã‚Šã�¾ã�™ã€‚
   - ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã�Œã€Œ2ã€�ã�§å§‹ã�¾ã�£ã�¦ã�„ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�
     Snort 2
     ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã‚’å®Ÿè¡Œã�—ã�¦ã�Šã‚Šã€�ã�“ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã‚’å�
   - ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã�Œã€Œ3ã€�ã�§å§‹ã�¾ã�£ã�¦ã�„ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�
     Snort 3
     ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã‚’å®Ÿè¡Œã�—ã�¦ã�Šã‚Šã€�ã�“ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã‚’å�

DNS ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã�Œæœ‰åŠ¹ã�«ã�ªã�£ã�¦ã�„ã‚‹ã�‹ã�©ã�†ã�‹ã‚’ç¢ºèª�

1. Cisco Defense Orchestrator Web ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ãƒã‚°ã‚¤ãƒ³ã�—ã�¾ã�™ã€‚
2. [ã‚¤ãƒ³ãƒ™ãƒ³ãƒˆãƒªï¼ˆInventoryï¼‰] ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã‚‰ é�©åˆ‡ã�ª FTD ãƒ‡ãƒ�ã‚¤ã‚¹ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚
3. [ç®¡ç�†ï¼ˆManagementï¼‰] é ˜åŸŸã�§ã€�[ãƒ�ãƒªã‚·ãƒ¼ï¼ˆPolicyï¼‰] ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
4. [è¨å®šï¼ˆSettingsï¼‰] ã‚¢ã‚¤ã‚³ãƒ³ï¼ˆæ¯è»Šã�®å½¢ï¼‰ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
5. [DNSãƒˆãƒ©ãƒ•ã‚£ãƒƒã‚¯ã�¸ã�®ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ï¼ˆReputation Enforcement on DNS trafficï¼‰] ã‚’ç¢ºèª�ã�—ã�¾ã�™ã€‚
   - è¨å®šã�Œã‚ªãƒ³ã�§ã�‚ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�¯ã�“ã�®è„†å¼±æ€§ã�®å½±éŸ
   - è¨å®šã�Œã‚ªãƒ•ã�§ã�‚ã‚‹å ´å�ˆã€�ãƒ‡ãƒ�ã‚¤ã‚¹ã�¯ã�“ã�®è„†å¼±æ€§ã�®å½±éŸ

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

ã�“ã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�®è„†å¼±æ€§ã�®ã�‚ã‚‹è£½å“�ã‚»ã‚¯ã‚·ãƒ§ãƒ³ã�«è¨˜è¼‰ã�•ã

ã‚·ã‚¹ã‚³ã�¯ã€�ã�“ã�®è„†å¼±æ€§ã�Œä»¥ä¸‹ã�®ã‚·ã‚¹ã‚³è£½å“�ã�«ã�¯å½±éŸ¿ã‚’ä¸Žã�ˆã�

- é�©å¿œåž‹ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ ã‚¢ãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹ï¼ˆASAï¼‰ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
- FMC ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
- Snort 2 ã‚’å®Ÿè¡Œã�—ã�¦ã�„ã‚‹ FTD ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
- Meraki MX ã‚·ãƒªãƒ¼ã‚º ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
- ã‚ªãƒ¼ãƒ—ãƒ³ã‚½ãƒ¼ã‚¹ã�® Snort 2 ãƒ—ãƒã‚¸ã‚§ã‚¯ãƒˆ
- ã‚ªãƒ¼ãƒ—ãƒ³ã‚½ãƒ¼ã‚¹ã�® Snort 3 ãƒ—ãƒã‚¸ã‚§ã‚¯ãƒˆ

å›žé�¿ç–

ã�“ã�®è„†å¼±æ€§ã�«å¯¾å‡¦ã�™ã‚‹å›žé�¿ç–ã�¯ã�‚ã‚Šã�¾ã�›ã‚“ã€‚ã�Ÿã� ã�—ã€�ç·©å’Œ DNS ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã‚’ç„¡åŠ¹ã�«ã�™ã‚‹ã�“ã�¨ã�Œã�§ã��ã�¾ã�™ã€‚FTD CLI ã�‹ã‚‰ DNS ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã‚’ç„¡åŠ¹ã�«ã�™ã‚‹æ–¹æ³•ã�¯ã€�ç®¡ç�†ãƒ‡ãƒ�ã‚¤ã‚¹ã�®è¨-

Cisco FMC ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã‚¤ã‚¹ã�® DNS ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã‚’ç„¡åŠ¹ã�«ã�™ã‚‹ã�«ã�¯ã€�æ¬¡ã�®æ‰‹é †ã‚’å®Ÿè¡Œã�—ã�

1. FMC Web ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ãƒã‚°ã‚¤ãƒ³ã�—ã�¾ã�™ã€‚
2. [ãƒ�ãƒªã‚·ãƒ¼ï¼ˆPoliciesï¼‰] ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã‚‰ [ã‚¢ã‚¯ã‚»ã‚¹åˆ¶å¾¡ï¼ˆAccess

Controlï¼‰] ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚

3. ç¢ºèª�ã�™ã‚‹ãƒ�ãƒªã‚·ãƒ¼ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚
4. [ç·¨é›†ï¼ˆEditï¼‰] ã‚¢ã‚¤ã‚³ãƒ³ï¼ˆé‰›ç†ã�®å½¢ï¼‰ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
5. [Advanced] ã‚¿ãƒ–ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
6. [å…¨èˆ¬è¨å®šï¼ˆGeneral Settingsï¼‰] ã�® [ç·¨é›†ï¼ˆEditï¼‰] ã‚¢ã‚¤ã‚³ãƒ³ï¼ˆé‰›ç†ã�®å½¢ï¼‰ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
7. [DNSãƒˆãƒ©ãƒ•ã‚£ãƒƒã‚¯ã�¸ã�®ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã‚’æœ‰åŠ¹ã�«ã�™ã‚‹ï¼ˆEna
   reputation enforcement on DNS trafficï¼‰]
   ãƒ�ã‚§ãƒƒã‚¯ãƒœãƒƒã‚¯ã‚¹ã‚’ã‚ªãƒ•ã�«ã�—ã�¦è¨å®šã‚’ã‚ªãƒ•ã�«ã�—ã�¾ã�™ã€‚
8. [OK] ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
9. å¤‰æ›´ã‚’ FTD ãƒ‡ãƒ�ã‚¤ã‚¹ã�«å±•é–‹ã�—ã�¾ã�™ã€‚

Cisco FDM ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã‚¤ã‚¹ã�® DNS ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã‚’ç„¡åŠ¹ã�«ã�™ã‚‹ã�«ã�¯ã€�æ¬¡ã�®æ‰‹é †ã‚’å®Ÿè¡Œã�—ã

1. FTD Web ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ãƒã‚°ã‚¤ãƒ³ã�—ã�¾ã�™ã€‚
2. ãƒ¡ã‚¤ãƒ³ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã‚‰ [ãƒ�ãƒªã‚·ãƒ¼ï¼ˆPoliciesï¼‰] ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
3. [ã‚¢ã‚¯ã‚»ã‚¹åˆ¶å¾¡ï¼ˆAccess Controlï¼‰]ã‚¿ãƒ–ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
4. [è¨å®šï¼ˆSettingsï¼‰] ã‚¢ã‚¤ã‚³ãƒ³ï¼ˆæ¯è»Šã�®å½¢ï¼‰ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
5. [DNSãƒˆãƒ©ãƒ•ã‚£ãƒƒã‚¯ã�¸ã�®ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ï¼ˆReputation Enforcement on DNS trafficï¼‰] ã‚’ç¢ºèª�ã�—ã�¾ã�™ã€‚
6. ã‚¹ã‚¤ãƒƒãƒ�ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¦è¨å®šã‚’ã‚ªãƒ•ã�«ã�—ã�¾ã�™ã€‚
7. [OK] ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚

Cisco Defense Orchestrator ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã‚¤ã‚¹ã�® DNS ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ã‚’ç„¡åŠ¹ã�«ã�™ã‚‹ã�«ã�¯ã€�æ¬¡ã�®æ‰‹é †ã‚’å®Ÿè¡Œã�—ã

1. Cisco Defense Orchestrator Web ã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ãƒã‚°ã‚¤ãƒ³ã�—ã�¾ã�™ã€‚
2. [ã‚¤ãƒ³ãƒ™ãƒ³ãƒˆãƒªï¼ˆInventoryï¼‰] ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã�‹ã‚‰ é�©åˆ‡ã�ª FTD ãƒ‡ãƒ�ã‚¤ã‚¹ã‚’é�¸æŠžã�—ã�¾ã�™ã€‚
3. [ç®¡ç�†ï¼ˆManagementï¼‰] **é ˜åŸŸã�§ã€�[ãƒ�ãƒªã‚·ãƒ¼ï¼ˆPolicyï¼‰]** ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
4. [è¨å®šï¼ˆSettingsï¼‰] ã‚¢ã‚¤ã‚³ãƒ³ï¼ˆæ¯è»Šã�®å½¢ï¼‰ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
5. [DNSãƒˆãƒ©ãƒ•ã‚£ãƒƒã‚¯ã�¸ã�®ãƒ¬ãƒ”ãƒ¥ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³é�©ç”¨ï¼ˆReputation Enforcement on DNS trafficï¼‰] ã‚’ç¢ºèª�ã�—ã�¾ã�™ã€‚
6. ã‚¹ã‚¤ãƒƒãƒ�ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¦è¨å®šã‚’ã‚ªãƒ•ã�«ã�—ã�¾ã�™ã€‚
7. [OK] ã‚’ã‚¯ãƒªãƒƒã‚¯ã�—ã�¾ã�™ã€‚
8. å¤‰æ›´ã‚’ FTD ãƒ‡ãƒ�ã‚¤ã‚¹ã�«å±•é–‹ã�—ã�¾ã�™ã€‚

ã�“ã‚Œã‚‰ã�®ç·©å’Œç–ã�¯åº‚Žå…¥ã�•ã‚Œã�¦ã�Šã‚Šã€�ãƒ†ã‚¹ãƒˆç’°å¢ƒã�§ã�¯å®Ÿè¨¼æ¸ˆã�

ä¿®æ£æ¸ˆã�¿ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢

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�Šå®¢æ§˜ã�Œã‚¤ãƒ³ã‚¹ãƒˆãƒ¼ãƒ«ã�—ã�Ÿã‚Šã‚µãƒ�ãƒ¼ãƒˆã‚’å�—ã�‘ã�Ÿã‚Šã�§ã��ã‚‹ã�®ã
ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ã�¨ãƒ•ã‚£ãƒ¼ãƒ�ãƒ£
ã‚»ãƒƒãƒˆã�«å¯¾ã�—ã�¦ã�®ã�¿ã�¨ã�ªã‚Šã�¾ã�™ã€‚ã��ã�®ã‚ˆã�†ã�ªã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

ã�¾ã�Ÿã€�ã�Šå®¢æ§˜ã�Œã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã‚’ãƒ€ã‚¦ãƒ³ãƒãƒ¼ãƒ‰ã�§ã��ã‚‹ã�®ã�¯ã€�ã‚
ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã�§ã�™ã€‚ç„¡å„Ÿã�®ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
ã‚¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã�«ã‚ˆã�£ã�¦ã€�ã�Šå®¢æ§˜ã�«æ–°ã�—ã�„ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
ãƒ©ã‚¤ã‚»ãƒ³ã‚¹ã€�è¿½åŠ ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ ãƒ•ã‚£ãƒ¼ãƒ�ãƒ£
ã‚»ãƒƒãƒˆã€�ã�¾ã�Ÿã�¯ãƒ¡ã‚¸ãƒ£ãƒ¼ ãƒªãƒ“ã‚¸ãƒ§ãƒ³
ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã�«å¯¾ã�™ã‚‹æ¨©é™�ã�Œä»˜ä¸Žã�•ã‚Œã‚‹ã�“ã�¨ã�¯ã�‚ã‚Šã�¾ã�

Cisco.com ã�® Cisco Support and Downloads
[ãƒšãƒ¼ã‚¸]()ã�«ã�¯ã€�ãƒ©ã‚¤ã‚»ãƒ³ã‚¹ã�¨ãƒ€ã‚¦ãƒ³ãƒãƒ¼ãƒ‰ã�«é–¢ã�™ã‚‹æƒ…å ±ã�Œè¨˜è¼‰ã�
Devicesï¼‰]
ãƒ„ãƒ¼ãƒ«ã‚’ä½¿ç”¨ã�™ã‚‹ã�Šå®¢æ§˜ã�®ã‚«ã‚¹ã‚¿ãƒžãƒ¼ãƒ‡ãƒ�ã‚¤ã‚¹ã‚µãƒ�ãƒ¼ãƒˆç¯„å›²ã‚‚è¡¨ç¤º

[ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã�®ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰]()ã‚’æ¤œè¨Žã�™ã‚‹éš›ã�«ã�¯ã€�[ã‚·ã‚¹ã‚³
ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒª
ãƒšãƒ¼ã‚¸]()ã�§å…¥æ‰‹ã�§ã��ã‚‹ã‚·ã‚¹ã‚³è£½å“�ã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã‚’å®šæœŸçš„ã�«å�‚ç
ã‚½ãƒªãƒ¥ãƒ¼ã‚·ãƒ§ãƒ³ä¸€å¼�ã‚’ç¢ºèª�ã�—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�ˆ†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�

ã‚µãƒ¼ãƒ“ã‚¹å¥‘ç´„ã‚’ã�”åˆ©ç”¨ã�§ã�ªã�„ã�Šå®¢æ§˜

ã‚·ã‚¹ã‚³ã�‹ã‚‰ç›´æŽ¥è³¼å…¥ã�—ã�Ÿã�Œã‚·ã‚¹ã‚³ã�®ã‚µãƒ¼ãƒ“ã‚¹å¥‘ç´„ã‚’ã�”åˆ©ç”¨ã�„ã�Ÿã�
[cisco-worldwide-
contacts.htmlï¼‰ã�«é€£çµ¡ã�—ã�¦ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã‚’å…¥æ‰‹ã�—ã�¦ã��ã� ã�•ã�,]()

ç„¡å„Ÿã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰ã�®å¯¾è±¡è£½å“�ã�§ã�‚ã‚‹ã�“ã�¨ã‚’è¨¼æ˜Žã�—ã�¦ã�„ã�Ÿã�
URL ã‚’ã�”ç”¨æ„�ã��ã� ã�•ã�„ã€‚

ä¿®æ£æ¸ˆã�¿ãƒªãƒªãƒ¼ã‚¹

æ¬¡ã�®è¡¨ã�§ã�¯ã€�å·¦ã�®åˆ—ã�«ã,·ã,¹ã,³ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ãƒªãƒªãƒ¼ã,¹ã,'è¨˜è¼‰ã�— è„†å¼±æ€§ã�®ã�„ã�šã,Œã�‹ã�«è©²å½"ã�™ã,‹ã�‹ã�©ã�†ã�‹ã€�ã�Šã,ˆã�³ã�� ã,Œã,‰ã

FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

Cisco FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã,¹	ã�"ã�®è„†å¼±æ€§ã�«å¯¾ã�™ã,‹æœ€åˆ�ã�®ä¿®æ£ãƒªãƒªãƒ¼ã,¹	ã,¢ãƒ‰
6.2.2 ä»¥å‰�[1]	è„†å¼±æ€§ã�ªã�—[2]	ä¿®æ£ã
6.2.3	è„†å¼±æ€§ã�ªã�—[2]	ä¿®æ£ã
6.3.0[1]	è„†å¼±æ€§ã�ªã�—[2]	ä¿®æ£ã
6.4.0	è„†å¼±æ€§ã�ªã�—[2]	6.4.0.15
6.5.01	è„†å¼±æ€§ã�ªã�—[2]	ä¿®æ£ã
6.6.0	è„†å¼±æ€§ã�ªã�—[2]	6.6.5.2
6.7.0	ä¿®æ£æ¸ˆã�¿ãƒªãƒªãƒ¼ã,¹ã�«ç§»è¡Œã�—ã�¾ã�™ã€,[3]	ä¿®æ£ã
7.0.0	7.0.2 (May 2022)	7.0.2 (M
7.1.0	7.1.0.1	7.1.0.1

1. Cisco FMC ã�Šã,ˆã�³ FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ 6.2.2 ä»¥å‰�ã�Šã,ˆã�³ 6.3.0ã€�6.5.0 ã�«ã�¤ã�„ã�¦ã�¯ã€� ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹ã�Œçµ‚ä°†ã�—ã�¦ã�„ã�¾ã�™ã€,ã�"ã�®è„†å¼±æ€§ã�
2. Cisco FDM ã�Šã,ˆã�³ Cisco Defense Orchestrator ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã,¤ã,¹ç"¨ã�«ã�¯ã€�Snort 3 ã�Œ Cisco FTD ãƒªãƒªãƒ¼ã,¹ 6.7.0 ã�«å^�ã,�ã�¦å�«ã�¾ã,Œã�¾ã�—ã�Ÿã€,Cisco FMC ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã,¤ã,¹ç"¨ã�«ã�¯ã€�Snort 3 ã�Œ Cisco FTD ãƒªãƒªãƒ¼ã,¹ 7.0.0 ã�§å^�ã,�ã�¦ãƒªãƒªãƒ¼ã,¹ã�•ã,Œã�¾ã�—ã�Ÿã€,
3.ãƒªãƒªãƒ¼ã,¹6.7.0ã�§ã�¯ã€�Cisco FDMã�Šã,ˆã�³Cisco Defense Orchestratorç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã,¤ã,¹ã�®ã�¿ã�Œè„†å¼±ã�§ã�™ã€,Snort 3ã�¯ãƒªãƒªãƒ¼ã,¹7.0.0ã�¾ã�§Cisco FMCç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã,¤ã,¹ã�§ãƒªãƒªãƒ¼ã,¹ã�•ã,Œã�¦ã�„ã�ªã�„ã�Ÿã,�ã€�Cisco FMCç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã,¤ã,¹ã�«ã�¯è„†å¼±æ€§ã�¯ã�,ã,Šã�¾ã�›ã,"ã€,

FTD ãƒ‡ãƒ�ã,¤ã,¹ã�®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰æ‰‹é †ã�«ã�¤ã�„ã�¦ã�¯ã€�Cisco Firepower Management Center ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,¬ã,¤ãƒ‰ã,'å�‚ç…§ã�—ã�¦ã��ã� ã�•ã�„ã€,

Product Security Incident Response Teamï¼ˆPSIRT; ãƒ—ãƒãƒ€ã,¯ãƒˆ ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¤ãƒ³ã,·ãƒ‡ãƒ³ãƒˆ ãƒ¬ã,¹ãƒ�ãƒ³ã,¹ ãƒ�ãƒ¼ãƒ ï¼‰ã�¯ã€�ã�“ã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�«è¨˜è¼‰ã�•ã‚Œã�¦ã�„ã‚‹è©²å½“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

å‡ºå…¸

ã�“ã�®è„†å¼±æ€§ã�¯ Cisco TAC
ã‚µãƒ�ãƒ¼ãƒˆã‚±ãƒ¼ã‚¹ã�®è§£æ±ºä¸ã�«ç™ºè¦‹ã�•ã‚Œã�¾ã�—ã�Ÿã€‚

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FTD-snort3-DOS-Aq38LVdM

æ”¹è¨‚å±¥æ´

ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³	èª¬æ˜Ž	ã‚»ã‚¯ã‚·ãƒ§ãƒ³	ã‚¹ãƒ†ãƒ¼ã‚¿ã‚¹	æ—¥ä»˜
1.0	åˆ�å›žå…¬é–‹ãƒªãƒªãƒ¼ã‚¹	-	Final	2022 å¹´ 4 æœˆ 27 æ—¥

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±¡

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。