è¤‡æ•°ã�®ã‚·ã‚¹ã‚³è£½å“�ã�®Snortãƒ«ãƒ¼ãƒ«

High

ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªãƒ¼ID : cisco-sa-snort-dos-RywH7ezM

å^�å…¬é–‹æ—¥ : 2021-10-27 16:00

ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ 1.0 : Final

CVSSã‚¹ã‚³ã‚¢ : 8.6

å›žé�¿ç– : Yes

Cisco ãƒ�ã‚° ID : CSCvy66065

CVE-2021-40116

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

æ¦‚è¦�

è¤‡æ•°ã�®ã‚·ã‚¹ã‚³è£½å“�ã�¯ã€�Snortãƒ«ãƒ¼ãƒ«ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã‚’å�—ã�‘ã�¾ã�

ã�“ã�®è„†å¼±æ€§ã�¯ã€�ãƒ«ãƒ¼ãƒ«ã�Œé�©å^‡ã�ªå^¶ç´„ã�ªã�—ã�§è¨å®šã�•ã‚Œã�¦ã�‚

æ³¨ï¼šSnort3ã�Œè¨å®šã�•ã‚Œã€�**Block with Reset**ã�¾ã�Ÿã�¯**Interactive Block with Resetã‚¢ã‚¯ã‚·ãƒ§ãƒ³ã�Œè¨å®šã�•ã‚Œã�¦ã�„ã‚‹ãƒ«ãƒ¼**ãƒ«ã�®ã�¿ã�Œè„†å¼±ã�§ã�™ã€‚Sno

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-RywH7ezM

ã�“ã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�¯ã€�Cisco ASAã€�FTDã€�ã�Šã‚ˆã�³ FMC ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒª ãƒ�ãƒ³ãƒ‰ãƒ«å…¬é–‹ã�® 2021 å¹´ 10 æœˆã�®ãƒªãƒªãƒ¼ã‚¹ã�®ä¸€éƒ¨ã�§ã�™ã€‚ã�“ã‚Œã‚‰ã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�¨ãƒªãƒ³ã‚¯ã�
ASAã€�FMCã€�ã�Šã‚ˆã�³FTDã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªãƒ�ãƒ³ãƒ‰

è©²å½“è£½å“�

è„†å¼±æ€§ã�®ã�‚ã‚‹è£½å“�

ã�“ã�®è„†å¼±æ€§ã�¯ã€�ãƒªãƒªãƒ¼ã‚¹3.1.0.100ã‚ˆã‚Šå‰�ã�®ã�™ã�¹ã�¦ã�®ã‚ªãƒ¼ãƒ—ã

ã‚·ã‚¹ã‚³è£½å“�ã�¸ã�®å½±éŸ¿

ã�“ã�®è„†å¼±æ€§ã�¯ã€�Cisco Firepower Threat

Defense(FTD)ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®è„†å¼±æ€§ã�Œå˜åœ¨ã�™ã,‹ãƒªãƒªãƒ¼ã,¹ã,'å®Ÿè¡Œã�—ã€

Firepower Threat Defense(FTD)ãƒ‡ãƒ�ã,¤ã,¹ã�¯ã€�Firepower Device Management(FDM)ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�«ã,ˆã�£ã�¦ç®¡ç�†ã�•ã,Œã€�ãƒªã,»ãƒƒãƒˆã,'ä¼´ã�†ãƒ

ã�"ã�®ãƒ‡ãƒ�ã,¤ã,¹ã�Œè„†å¼±ã�«ã�ªã,‹ã�«ã�¯ã€�Firewall Management Center(FMC)ç®¡ç�†å¯¾è±¡ãƒ‡ãƒ�ã,¤ã,¹ã�®3ã�¤ã�®æ�¡ä»¶ã�Œæº€ã�Ÿã�•ã,Œã�¦ã�„ã,‹

- ãƒ‡ãƒ�ã,¤ã,¹ã�¯Snort3ã,'å®Ÿè¡Œã�—ã�¦ã�„ã,‹å¿…è¦�ã�Œã�,ã,Šã�¾ã�™ã€,
- ãƒ‡ãƒ�ã,¤ã,¹ã�«ã�¯ã€�[ãƒªã,»ãƒƒãƒˆã,'å�«ã,€ãƒ–ãƒãƒƒã,¯]ã�¾ã�Ÿã�¯[ãƒªã,»ãƒƒãƒˆã,'å�
- **Reset**ã,¢ã,¯ã,·ãƒ§ãƒ³ã�§è¨å®šã�•ã,Œã�Ÿãƒ«ãƒ¼ãƒ«**ã�¯ã€�**ãƒ«ãƒ¼ãƒ«å†…ã�®ã,¢ãƒ—ãƒªã,±

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

FTDè¨å®šã�®æ±ºå®š

Snort3ã�Œè¨å®šã�•ã,Œã�¦ã�„ã,‹ã�‹ã�©ã�†ã�‹ã,'ç¢ºèª�ã�™ã,‹ã�«ã�¯

1. FMC Webã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã�«ç§»å‹•ã�—ã�¾ã�™ã€,
2. [Devices]ãƒšãƒ¼ã,¸ã�«ç§»å‹•ã�—ã€�[**Device Management**]ã,¿ãƒ–ã�«ç§»å‹•ã�—ã�¾ã�™ã€,
3. ç¢ºèª�ã�™ã,‹FTDãƒ‡ãƒ�ã,¤ã,¹ã,'é�¸æŠžã�—ã�¾ã�™ã€,[Edit] ã,'é�¸æŠžã�—ã�¾ã�™ã€,
4. [Device]ã,¿ãƒ–ã�«ç§»å‹•ã�—ã€�[Inspection Engine]é ˜åŸŸã,'ç¢ºèª�ã�—ã�¾ã�™ã€,
5. ã�"ã,Œã�«ã,ˆã,Šã€�Snort2ã�¾ã�Ÿã�¯Snort 3ã�Œãƒªã,¹ãƒˆã�•ã,Œã�¾ã�™ã€,
   - Snort2ã�Œãƒªã,¹ãƒˆã�•ã,Œã�¦ã�„ã,‹å ´å�ˆã€�ãƒ‡ãƒ�ã,¤ã,¹ã�«ã�¯è„†å¼±æ€§ã�¯
   - Snort3ã�Œãƒªã,¹ãƒˆã�•ã,Œã�¦ã�„ã,‹å ´å�ˆã€�ãƒ‡ãƒ�ã,¤ã,¹ã�«è„†å¼±æ€§ã�Œå˜å

[ãƒªã,»ãƒƒãƒˆã,'å�«ã,€ãƒ–ãƒãƒƒã,¯]ã,¢ã,¯ã,·ãƒ§ãƒ³ã�¾ã�Ÿã�¯[ãƒªã,»ãƒƒãƒˆã,'å�«ã,€ã,¤ãƒ³ã

1. FMC Webã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã,§ã,¤ã,¹ã�«ç§»å‹•ã�—ã�¾ã�™ã€,
2. [Policies]ãƒšãƒ¼ã,¸**ã�«ç§»å‹•**ã�—ã€�[**Access Control**]**ã,¿ãƒ–ã�«ç§»å‹•**ã�—ã�¾ã�™ã€,
3. ç¢ºèª�ã�™ã,‹ãƒ�ãƒªã,·ãƒ¼ã,'é�¸æŠžã�—ã€�[**Edit**]ã,'é�¸æŠž**ã�—ã�¾ã�**™ã€,
4. ã��ã�®ãƒ�ãƒªã,·ãƒ¼ã�®å�„ãƒ«**ãƒ¼ãƒ«ã�®[**ã,¢ã,¯ã,·ãƒ§ãƒ³]åˆ—ã�®ä¸‹ã,'ç¢ºèª�ã�—ã�
   - [ãƒªã,»ãƒƒ**ãƒˆä»˜ã��ãƒ–ãƒãƒƒ**ã,¯]ã�¾ã�Ÿã�¯[ãƒªã,»**ãƒƒãƒˆä»˜ã��ã,¤ãƒ³ã,¿ãƒ©ã,¯ãƒ†**
   - ã,¢ã,¯ã,·ãƒ§ãƒ³ã�®ä¸‹**ã�«[ãƒªã,»ãƒƒãƒˆä»˜ã��ãƒ–ãƒãƒƒ**ã,¯]ã�¾ã�Ÿã�¯[ãƒªã,»**ãƒƒãƒ**

ãƒªã,»ãƒƒãƒˆã,¢ã,¯ã,·ãƒ§ãƒ³ã,'å�«ã,€ãƒ«ãƒ¼ãƒ«ã�«è„†å¼±æ€§ã�®ã�,ã,‹è¨å®šã�Œã�,ã,‹ã�

ãƒ‡ãƒ�ã‚¤ã‚¹ã�ŒSnort3ã‚'å®Ÿè¡Œã�—ã€�**Block with Reset**ã‚¢ã‚¯ã‚·ãƒ§ãƒ³ã�¾ã�Ÿã�¯**Interactive Block with Resetã‚¢ã‚¯ã‚·ãƒ§ãƒ³ã�Œè¨å®šã�•ã‚Œã�¦ã�„ã‚‹å ´å�ˆ**ã�¯ã€�ãƒ«ãƒ¼ãƒ«ã�Œè„†å¼±ã�ªæ§‹

æ¬¡ã�®è¡¨ã�¯ã€�FMCã�§è¡¨ç¤ºã�•ã‚Œã‚‹FTDãƒ‡ãƒ�ã‚¤ã‚¹ã�®è¨å®šæƒ…å ±ã‚'ç¤ºã�—ã�¦ã

è„†å¼±æ€§ã�®å˜åœ¨ã�™ã‚‹ã‚³ãƒ³ãƒ•ã‚£ã‚®ãƒ¥ãƒ¬ãƒ¼ã‚·ãƒ§ãƒ³

ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³ã�¾ã�Ÿã�¯ãƒ—ãƒãƒˆã‚³ãƒ«ï¼ˆTCPã�¾ã�Ÿã�¯UDPï¼‰ã‚'å'¼ã�³å‡ºã

è„†å¼±æ€§ã�®ã�‚ã‚‹è¨å®šã‚'å�«ã‚€ãƒ«ãƒ¼ãƒ«ã�®ä¾‹ã‚'æ¬¡ã�«ç¤ºã�—ã�¾ã�™

ãƒ«ãƒ¼ãƒ«å��	ã‚½ãƒ¼ã‚¹ã‚¾ãƒ¼ãƒ³	å®›å…ˆã‚¾ãƒ¼ãƒ³	ã‚½ãƒ¼ã‚¹ãƒ�ãƒƒãƒˆãƒ¯ãƒ¼ã‚¯	å®›å…ˆãƒ
Ex1	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�
Ex2	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�

è„†å¼±æ€§ã�®ã�ªã�„è¨å®š

ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³ã�¾ã�Ÿã�¯ãƒ—ãƒãƒˆã‚³ãƒ«ï¼ˆTCPã�¾ã�Ÿã�¯UDPï¼‰ã‚'å'¼ã�³å‡ºã

ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³ãƒ†ãƒ³ãƒ—ãƒ¬ãƒ¼ãƒˆã�¨ä¾‹

æ¬¡ã�«ã€�ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³ã‚'å'¼ã�³å‡ºã�™è„†å¼±æ€§ã�®ã�ªã�„è¨å®šã�®ãƒ†ãƒ³

ãƒ«ãƒ¼ãƒ«å��	ã‚½ãƒ¼ã‚¹ã‚¾ãƒ¼ãƒ³	å®›å…ˆã‚¾ãƒ¼ãƒ³	ã‚½ãƒ¼ã‚¹ãƒ�ãƒƒãƒˆãƒ¯ãƒ¼ã‚¯	å®›å…ˆãƒ
Ex1	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�
Ex2	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�

æ¬¡ã�«ã€�ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³ã‚'å'¼ã�³å‡ºã�™è„†å¼±æ€§ã�®ã�ªã�„è¨å®šã�®ä¾‹ã‚'

ãƒ«ãƒ¼ãƒ«å��	ã‚½ãƒ¼ã‚¹ã‚¾ãƒ¼ãƒ³	å®›å…ˆã‚¾ãƒ¼ãƒ³	ã‚½ãƒ¼ã‚¹ãƒ�ãƒƒãƒˆãƒ¯ãƒ¼ã‚¯	å®›å…ˆãƒ
Ex1	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�
Ex2	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�

ãƒ—ãƒãƒˆã‚³ãƒ«ãƒ†ãƒ³ãƒ—ãƒ¬ãƒ¼ãƒˆã�¨ä¾‹

ãƒ—ãƒãƒˆã‚³ãƒ«ï¼ˆTCPã�¾ã�Ÿã�¯UDPï¼‰ã‚'å'¼ã�³å‡ºã�™è„†å¼±æ€§ã�®ã�ªã�„è¨å®šã�®
ã�"ã�®ä¾‹ã�¯ã€�å¿…è¦�ã�ªæœ€å°�æ§‹æˆ�ã‚'ç¤ºã�—ã�¦ã�„ã�¾ã�™ã€‚

ãƒ«ãƒ¼ãƒ«å��	ã‚½ãƒ¼ã‚¹ã‚¾ãƒ¼ãƒ³	å®›å…ˆã‚¾ãƒ¼ãƒ³	ã‚½ãƒ¼ã‚¹ãƒ�ãƒƒãƒˆãƒ¯ãƒ¼ã‚¯	å®›å…ˆãƒ
Ex1	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�

ãƒ«ãƒ¼ãƒ«å��	ã,½ãƒ¼ã,¹ã,¾ãƒ¼ãƒ³	å®›å…ˆã,¾ãƒ¼ãƒ³	ã,½ãƒ¼ã,¹ãƒ�ãƒƒãƒˆãƒ¯ãƒ¼ã,¯	å®›å…ˆãƒ
Ex2	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�

æ¬¡ã�«ã€�ãƒ—ãƒãƒˆã,³ãƒ«ï¼ˆTCPã�¾ã�Ÿã�¯UDPï¼‰ã,'å'¼ã�³å‡ºã�™è„†å¼±æ€§ã�®ã�ªã
ã�"ã�®ä¾‹ã�¯ã€�å¿…è¦�ã�ªæœ€å°�æ§‹æˆ�ã,'ç¤ºã�—ã�¦ã�„ã�¾ã�™ã€,

ãƒ«ãƒ¼ãƒ«å��	ã,½ãƒ¼ã,¹ã,¾ãƒ¼ãƒ³	å®›å…ˆã,¾ãƒ¼ãƒ³	ã,½ãƒ¼ã,¹ãƒ�ãƒƒãƒˆãƒ¯ãƒ¼ã,¯	å®›å…ˆãƒ
Ex1	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�
Ex2	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�
Ex3	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�
Ex4	ä»»æ„�	ä»»æ„�	ä»»æ„�	ä»»æ„�

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�Œã,ªãƒ¼ãƒ—ãƒ³ã,½ãƒ¼ã,¹ã�®Snort2ãƒ—ãƒã,¸ã,§ã,¯ãƒˆã�

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,¢
- 1000 ã,·ãƒªãƒ¼ã,º ã,µãƒ¼ãƒ"ã,¹çµ±å�ˆåž‹ãƒ«ãƒ¼ã,¿ï¼ˆISRï¼‰
- 4000 ã,·ãƒªãƒ¼ã,º ã,µãƒ¼ãƒ"ã,¹çµ±å�ˆåž‹ãƒ«ãƒ¼ã,¿ï¼ˆISRï¼‰
- Catalyst 8000V ã,¨ãƒƒã,¸ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
- Catalyst 8200 ã,·ãƒªãƒ¼ã,º ã,¨ãƒƒã,¸ ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ
- Catalyst 8300 ã,·ãƒªãƒ¼ã,º ã,¨ãƒƒã,¸ ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ
- Catalyst 8500 ã,·ãƒªãƒ¼ã,º ã,¨ãƒƒã,¸ ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ
- Catalyst 8500L ã,·ãƒªãƒ¼ã,º ã,¨ãƒƒã,¸ ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ
- Cloud Services Router 1000V ã,·ãƒªãƒ¼ã,º
- Firepower Management Centerï¼ˆFMCï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
- ã,µãƒ¼ãƒ"ã,¹çµ±å�ˆåž‹ä»®æƒ³ãƒ«ãƒ¼ã,¿ï¼ˆISRvï¼‰
- Meraki MX ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹

å›žé�¿ç–

ã�"ã�®è„†å¼±æ€§ã�«å¯¾å‡¦ã�™ã,‹å›žé�¿ç–ã�Œã�,ã,Šã�¾ã�™ã€,

ã�"ã,Œã,‰ã�®å›žé�¿ç–ã�¯å°Žå…¥ã�•ã,Œã€�ãƒ†ã,¹ãƒˆç'°å¢ƒã�§æˆ�åŠŸã�—ã�Ÿã�"ã�¨ã�

æ³¨ï¼šã�"ã�®å•�é¡Œã�«ã�¯3ã�¤ã�®å›žé�¿ç–ã�Œã�,ã,Šã�¾ã�™ã€,å›žé�¿ç–ã,'å®Ÿè£…ã�

å›žé�¿ç– 1

æœ€åˆ�ã�®å›žé�¿ç–ã�¯ã€�Snortã‚¤ãƒ³ã‚¹ãƒšã‚¯ã‚·ãƒ§ãƒ³ã‚¨ãƒ³ã‚¸ãƒ³ã‚'Snort3ã�‹ã‚‰Snort2ã�«å
æ½œåœ¨çš„ã�ªå½±éŸ¿ã�«ã�¤ã�„ã�¦ã�¯ã€�è¨å®šã‚¬ã‚¤ãƒ‰ã�¾ã�Ÿã�¯ã‚µãƒ�ãƒ¼ãƒˆãƒ

1. FMC Webã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ç§»å‹•ã�—ã�¾ã�™
2. [ãƒ‡ãƒ�ã‚¤ã‚¹]ãƒšãƒ¼ã‚¸ã�«ç§»å‹•ã�—ã€�[ãƒ‡ãƒ�ã‚¤ã‚¹ç®¡ç�†]ã‚¿ãƒ–ã�«ç§»å‹•ã�—ã�¾ã
3. ç¢ºèª�ã�™ã‚‹FTDãƒ‡ãƒ�ã‚¤ã‚¹ã‚'é�¸æŠžã�—ã�¾ã�™ã€‚[Edit] ã‚'é�¸æŠžã�—ã�¾ã�™ã€‚
4. [Device]ã‚¿ãƒ–ã�«ç§»å‹•ã�—ã€�[Inspection Engine]é ˜åŸŸã‚'ç¢ºèª�ã�—ã�¾ã�™ã€‚
5. ã€ŒSnort2ã�«æˆ»ã�™ã€�ã‚ªãƒ—ã‚·ãƒ§ãƒ³ã‚'é�¸æŠžã�—ã�¾ã�™ã€‚

å›žé�¿ç– 2

2ã�¤ç›®ã�®å›žé�¿ç–ã�¯ã€�ã�™ã�¹ã�¦ã�®ãƒ«ãƒ¼ãƒ«ã‚¢ã‚¯ã‚·ãƒ§ãƒ³ã‚'[ãƒªã‚»ãƒƒãƒˆä»˜ã��ã

1. FMC Webã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ã‚¤ã‚¹ã�«ç§»å‹•ã�—ã�¾ã�™
2. [Policies]ãƒšãƒ¼ã‚¸ã�«ç§»å‹•ã�—ã€�[Access Control]ã‚¿ãƒ–ã�«ç§»å‹•ã�—ã�¾ã�™ã€‚
3. ç¢ºèª�ã�™ã‚‹ãƒ�ãƒªã‚·ãƒ¼ã‚'é�¸æŠžã�—ã€�[Edit]ã‚'é�¸æŠžã�—ã�¾ã�™ã€‚
4. ãƒªã‚»ãƒƒãƒˆæ“�ä½œã‚'å�«ã‚€ãƒ«ãƒ¼ãƒ«ã‚'æ¤œç´¢ã�—ã€�[Edit]ã‚'é�¸æŠžã�—ã�¾ã�™ã€‚
5. ã‚¢ã‚¯ã‚·ãƒ§ãƒ³ã‚'[ãƒªã‚»ãƒƒãƒˆä»˜ã��ãƒ–ãƒãƒƒã‚¯]ã�¾ã�Ÿã�¯[ãƒªã‚»ãƒƒãƒˆä»˜ã��ã‚¤ãƒ³ã‚¿ãƒ

å›žé�¿ç– 3

3ç•ªç›®ã�®å›žé�¿ç–ã�¯ã€�ãƒ•ã‚¡ã‚¤ã‚¢ã‚¦ã‚©ãƒ¼ãƒ«ãƒªã‚»ãƒƒãƒˆãƒ«ãƒ¼ãƒ«ã‚'çµžã‚Šè¾¼ã‚“ã�§ã€�

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„¡
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�

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�†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�"å�ˆ©ç"¨ã�§ã�ªã�„ã�Šå®¢æ§˜

ã,·ã,¹ã,³ã�‹ã,‰ç›´æŽ¥è³¼å…¥ã�—ã�Ÿã�Œ Cisco Service Contract
ã,'ã�"å�ˆ©ç"¨ã�„ã�Ÿã� ã�„ã�¦ã�„ã�ªã�„å ´å�ˆã€�ã�¾ã�Ÿã€�ã,µãƒ¼ãƒ‰ãƒ'ãƒ¼ãƒ†ã,£ãƒ™
POS ã�‹ã,‰å…¥æ‰‹ã�§ã��ã�ªã�„å ´å�ˆã�¯ã€�Cisco TAC
ã�«é€£çµ¡ã�—ã�¦ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,'å…¥æ‰‹ã�—ã�¦ã��ã� ã�•ã�„ã€,https://www.ci
cisco-worldwide-contacts.html

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�«ç¤ºã�™ã,ˆã�†ã�«ã€�è©²å½"ã�™ã,‹ä¿®æ£æ¸ˆã�¿ã�®ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ

Cisco FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

æ¬¡ã�®è¡¨ã�§ã�¯ã€�å·¦ã�®åˆ—ã�«ã,·ã,¹ã,³
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ãƒªãƒªãƒ¼ã,¹ã,'è¨˜è¼‰ã�—ã�¦ã�„ã�¾ã�™ã€,ä¸å¤®ã�®åˆ—ã�¯ã€�ãƒª
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

FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹	ã�"ã�®è„†å¼±æ€§ã�«å¯¾ã�™ã,‹æœ€å�ˆ�ã�®ä¿®æ£ãƒªã
6.2.2 ä»¥å‰�[1]	è„†å¼±æ€§ã�ªã�—
6.2.3	è„†å¼±æ€§ã�ªã�—
6.3.0[1]	è„†å¼±æ€§ã�ªã�—
6.4.0	è„†å¼±æ€§ã�ªã�—
6.5.01	è„†å¼±æ€§ã�ªã�—
6.6.0	è„†å¼±æ€§ã�ªã�—
6.7.02	è„†å¼±æ€§ã�ªã�—
7.0.0	7.0.1

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‚äº†ã�—ã�¦ã�„ã�¾ã�™ã€‚ã�“ã�®è„†å¼±æ€§ã�

2.

Snort3ã‚¤ãƒ³ã‚¹ãƒšã‚¯ã‚·ãƒ§ãƒ³ã‚¨ãƒ³ã‚¸ãƒ³ã�®ã‚ªãƒ—ã‚·ãƒ§ãƒ³ã�¯ã€�6.7.0ã�®FDMã�Œç®¡ç�†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€‚

ã‚ªãƒ¼ãƒ—ãƒ³ã‚½ãƒ¼ã‚¹ã�® Snort

ã‚ªãƒ¼ãƒ—ãƒ³ã‚½ãƒ¼ã‚¹ã�® Snort ã�®è©³ç´°ã�«ã�¤ã�„ã�¦ã�¯ã€�Snort ã�® Web ã‚µã‚¤ãƒˆã‚’å�‚ç…§ã�—ã�¦ã��ã� ã�•ã�„ã€‚

Snortãƒªãƒªãƒ¼ã‚¹	ã�“ã�®è„†å¼±æ€§ã�«å¯¾ã�™ã‚‹æœ€å^�ã�®ä¿®æ£ãƒªãƒªãƒ¼ã‚¹
2.x	è„†å¼±æ€§ã�ªã�—
3.x	3.1.0.100

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£å^©ç”¨äº‹ä¾‹ã�¨å…¬å¼�ç™ºè¡¨

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-RywH7ezM

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	å^�å›žå…¬é–‹ãƒªãƒªãƒ¼ã‚¹	â€”	æœ€çµ‚ç‰ˆ	2021 å¹´ 10 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±¡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。