è¤‡æ•°ã�®ã,·ã,¹ã,³è£½å“�ã�«ã�Šã�'ã,‹Snort TCP Fast Open File ãƒ‘ãƒ¼ã,·ãƒ¼ãƒ‘ã,¤ãƒ'ã,¹ã�®è„†å¼±æ€§

Medium

ã,¢ãƒ‰ãƒ‘ã,¤ã,¶ãƒªãƒ¼ID : cisco-sa-snort-tfo-bypass-MmzZrtes

CVE-2021-1224

åˆ�å...¬é–‹æ—¥ : 2021-01-13 16:00

æœ€çµ‚æ›´æ–°æ—¥ : 2021-05-20 13:27

ãƒ‘ãƒ¼ã,¸ãƒ§ãƒ³ 1.2 : Final

CVSSã,¹ã,³ã,¢ : 5.8

å›žé¿ç– : Yes

Cisco ãƒ‘ã,° ID : CSCvt43136 CSCvu88532

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

æ¦,è¦

Snortæ¤œå‡ºã,¨ãƒ³ã,¸ãƒ³ã�¨çµ„ã�¿å�ˆã,�ã�›ã�¦ä½¿ç"¨ã™ã,‹å ´å�ˆã€�è¤‡æ•°ã�®ã,·ã,¹ã,³è£½å Fast Open(TFO)ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã,'å�—ã�'ã�¾ã�™ã€,ã�"ã�®è„†å¼±æ€§ã�«ã,ˆã,Šã€�è

ã�"ã�®è„†å¼±æ€§ã�¯ã€�å°'ã�ªã��ã��ã�¨ã,,éƒ¨å^†çš„ã�«TFOæŽ¥ç¶šãƒ‘ãƒ³ãƒ‰ã,·ã,§ã,¤ã,¯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€¯æ¬¡ã�®ãƒªãƒ³ã,¯ã,ˆã,Šç¢ºèª�ã�§ã��ã��ã€,
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes

è©²å½“è£½å“�

è„†å¼±æ€§ã�®ã�,ã,‹è£½å“�

ã�"ã�®è„†å¼±æ€§ã�®å...¬é–‹æ™,ç,¹ã�§ã€�ã,·ã,¹ã,³ã�®ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®æœ€å^�ã�®

- 3000 ã,·ãƒªãƒ¼ã,ºç”£æ¥ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ï¼^ISAï¼‰
- Firepower Threat Defenseï¼^FTDï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
- Meraki MX64
- Meraki MX64W

- Meraki MX67
- Meraki MX67C
- Meraki MX67W
- Meraki MX68
- Meraki MX68CW
- Meraki MX68W
- Meraki MX84
- Meraki MX100
- Meraki MX250
- Meraki MX450

å…¬é–‹æ™‚ç‚¹ã§IOS XEç”¨ã®Cisco UTD Snort IPSã,¨ãƒ³ã,¸ãƒ³ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã¾ã€Ÿã¯IOS XE SD-WANã,½ãƒ•ãƒˆã,¦ã,§ã,¢ç”¨ã®Cisco UTDã,¨ãƒ³ã,¸ãƒ³ã®æœ€å^€ã®ä¿®æ£æ¸ˆã¿ãƒªãƒªãƒ¼ã,¹ã,^ã,Šã,,å‰€ã®ãƒªãƒªãƒ¼ã,¹ã,'å®

- 1000 ã,·ãƒªãƒ¼ã,º ã,µãƒ¼ãƒ“ã,¹çµ±å€^åž‹ãƒ«ãƒ¼ã,¿ï¼^ISRï¼‰
- 4000 ã,·ãƒªãƒ¼ã,º ISR
- 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 8500Lã,¨ãƒƒã,¸ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ
- Cloud Services Router 1000V(CSR 1000V)
- ã,µãƒ¼ãƒ“ã,¹çµ±å€^åž‹ä»®æƒ³ãƒ«ãƒ¼ã,¿ï¼^ISRvï¼‰

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‰ãƒã,¤ã,¶ãƒªã€®ã€Œä ID ã®è©³ç´°ã,»ã,¯ã,·ãƒ§ãƒ³ã,'å€,ç…§ã—ã—¦ã••ã• ã••ã„€,

å…¬é–‹æ™‚ç‚¹ã§ã¯ã€“ã®è„†å¼±æ€§ã¯ãƒªãƒªãƒ¼ã,¹2.9.17ã,^ã,Šå‰€ã®ã®ã™ã¹ã

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

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

ã,·ã,¹ã,³ã¯ã€“ã®è„†å¼±æ€§ã•Œä»¥ä¸‹ã®ã,·ã,¹ã,³è£½å“•ã«ã¯å½±éŸ¿ã,'ä¸Žã•^ã•

- é•©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ï¼^ASAï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
- Catalyst 8500ã,¨ãƒƒã,¸ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ
- Firepower Management Centerï¼^FMCï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
- Meraki vMX100ä»®æƒ³ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹
- Meraki Z1ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹
- Meraki Z3ã,·ãƒªãƒ¼ã,ºã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹

å›žé¿ç–

ã"ã®å›žé¿ç–ã¯å°Žå…¥ã•ã,Œã¦ã¦ã‰ã,Šã€ãƒ†ã,¹ãƒˆç'°å¢ƒã§ã¯å®Ÿè¨¼æ¸ˆã¿ã¿ã§ã

Cisco FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹6.7.0

Cisco FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹6.7.0ã§ã¯ã€Snort
3è¨å®šã,ªãƒ—ã,·ãƒ§ãƒ³ã‚Œæœ‰åŠ¹ã«ã«ãªã£ã¦ã„ã‚‹å ´å^ã®å›žé¿ç–¨ã¨ã—ã¦ã

æ¬¡ã®æ‰‹é †ã,'ä½¿"¨ã—ã¦ã€Snort
3ã®è¨å®šã,ªãƒ—ã,·ãƒ§ãƒ³ã‚Œæœ‰åŠ¹ã«ã«ãªã£ã¦ã„ã‚‹ã‚‹ã"ã¨ã,'ç¢ºèªã—ã¾ã™ã
Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version
6.7ã€ã®ã€Œ*Snort 2ã¨Snort*
*3ã®å^‡ã,Šæ›¿ã^ã€ã,»ã,¯ã,·ãƒ§ãƒ³ã,'å,ç…§ã—ã¦ã••ã ã•ã„ã€,

1. FTDå°Žå…¥ã®ç®¡ç†ãƒ–ãƒ¼ã,¿ãƒ«ã««ãƒã,¤ãƒ³ã—ã¾ã™ã€,
2. [Policies] > [Intrusion] ã««ç§»å‹•ã—ã¾ã™ã€,
3. ãƒ†ãƒ¼ãƒ–ãƒ«ã®ä¸Šã««ã,‹**Snort**
   Versionè¡Œã,'æŽ¢ã—ã¾ã™ã€,ç¾åœ¨ã®ãƒ–ãƒ¼ã,¸ãƒ§ãƒ³ã¯ã€å®Œå…¨ãªãƒãƒ
   95ã¯Snort 2ã®ãƒ–ãƒ¼ã,¸ãƒ§ãƒ³ã§ã™ã€,

ãƒ«ãƒ¼ãƒ«129:2ã,'æœ‰åŠ¹ã«ã™ã,‹ã«ã¯ã€æ¬¡ã®æ‰‹é †ã,'å®Ÿè¡Œã—ã¾ã™ã€,è©³ç´
Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version
6.7ã€ã®ã€Œ*Changing Intrusion Rule Actions(Snort*
*3)*ã€ã,»ã,¯ã,·ãƒ§ãƒ³ã,'å,ç…§ã—ã¦ã••ã ã•ã„ã€,

1. FTDå°Žå…¥ã®ç®¡ç†ãƒ–ãƒ¼ã,¿ãƒ«ã««ãƒã,¤ãƒ³ã—ã¾ã™ã€,
2. [Policies] > [Intrusion] ã««ç§»å‹•ã—ã¾ã™ã€,
3. [Balanced Security and Connectivity]
   ã•ã©ã®ã,·ã,¹ãƒ†ãƒ æ••ä¾›ãƒ–ãƒªã,·ãƒ¼ã,'é¸æŠžã—ã¾ã™ã€,
4. ãƒ«ãƒ¼ãƒ«**129:2**ã,'æ¤œç´¢ã—ã¾ã™ã€,
5. ãƒ«ãƒ¼ãƒ«ã,'有åŠ¹ã«ã™ã,‹ã«ã¯ã€ãƒ«ãƒ¼ãƒ«ã®æ¨ªã«ã,‹ãƒ»ã,§ãƒƒã,¯ãƒœãƒ
6. [Action] ãƒ‰ãƒãƒƒãƒ—ãƒ€ã,¦ãƒ³ãƒªã,¹ãƒˆã‹ã,‰[Drop] ã,'é¸æŠžã—ã¾ã™ã€,
7. **ã,¢ã,¯ã,»ã,¹ã,³ãƒ³ãƒˆãƒ¼ãƒ«ãƒ»ãƒ¼ã**ã§ã€ä¾µå…¥ãƒãƒªã,·ãƒ¼ã,'ãƒ«ãƒ¼ãƒ«ã«è¿½åŠ

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,‹éš›ã«ã¯ã€ã,·ã,¹ã,³
ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ‰ãƒã,¤ã,¶ãƒª
ãƒšãƒ¼ã,¸ã§å…¥æ‰‹ã§ã,‹ã,·ã,¹ã,³è£½å“ã®ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã,'å®šæœŸçš„ã«å,ç
ã,½ãƒªãƒ¥ãƒ¼ã,·ãƒ§ãƒ³ä¸€å¼ã,'ç¢ºèªã—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€€åˆ†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€«

ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã,¹

å…¬é–‹æ™‚ç‚¹ã€§ã€¯ã€“ã€®è„†å¼±æ€§ã®å½±éŸ¿ã,’å€—ã€‘ã,‹è£½å“€ã€«ã€¤ã€„ã€¦
ID
ã€®è©³ç´°ã,»ã,¯ã,·ãƒ§ãƒ³ã,’å€,ç…§ã€—ã€¦ã€€ã€•ã€„ã€,ã,ªãƒ¼ãƒ—ãƒ³ã,½ãƒ¼ã,¹ã€®Snortã

- Snort 2ã,ªãƒ—ã,·ãƒ§ãƒ³ã€Œè¨å®šã€•ã,Œã€¦ã€„ã,‹å ´å€ˆã€€Cisco FTDãƒªãƒªãƒ¼ã,¹6.4.0.12ã€€6.6.3ã€€ã€Šã,^ã€³6.7.0ä»¥é™€ã€«ã€¯ã€€ã€“ã€®è„†å¼±æ€
- Cisco FTDãƒªãƒªãƒ¼ã,¹6.7.0ä»¥é™€ã€¯ã€€Snort 3ã,ªãƒ—ã,·ãƒ§ãƒ³ã€Œè¨å®šã€•ã,Œã€€ãƒ«ãƒ¼ãƒ«129:2ã€Œãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ã,’ãƒ‰ãƒãƒƒãƒ—
- IOS XE 16.12.5ã€€17.3.3ã€€ã€Šã,^ã€³17.4.1[1]ç”¨ã€®Cisco UTD Snort IPSã,¨ãƒ³ã,¸ãƒ³ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€«ã€¯ã€€ã€“ã€®è„†å¼±æ€§ã€«å¯¾ã€™ã,‹ä¿®æ£ã€Œ
- ã,·ã,¹ã,³ã€§ã€¯ã€€Meraki MXã,·ãƒªãƒ¼ã,°ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ã€®ã€“ã€®è„†å¼±æ€§ã€«å¯¾å‡¦ã€
- ã,ªãƒ¼ãƒ—ãƒ³ã,½ãƒ¼ã,¹ã€®Snortãƒ—ãƒã,¸ã,§ã,¯ãƒˆã€®ãƒªãƒªãƒ¼ã,¹2.9.17ä»¥é™€ã€«ã€¯ã€€
- ã,ªãƒ¼ãƒ—ãƒ³ã,½ãƒ¼ã,¹ã€®Snortãƒ—ãƒã,¸ã,§ã,¯ãƒˆã€®ãƒªãƒªãƒ¼ã,¹3.0ä»¥é™€ã€¯ã€€ãƒ«ãƒ¼ã

  1. 17.2.1ä»¥é™€ã€€Cisco IOS XEã€Šã,^ã€³IOS XE SD-WANã€¯å€Œã€˜ã,¤ãƒ¡ãƒ¼ã,¸ãƒ•ã,¡ã,¤ãƒ«ã,’ä½¿ç”¨ã€—ã€¾ã€™ã€,

ä¸€æ£åˆ©ç”¨äº‹ä¾‹ã€¯å…¬å¼€ç™ºè¡¨

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

å‡ºå…¸

ã,·ã,¹ã,³ã€¯ã€€ã€“ã€®è„†å¼±æ€§ã,’å ±å‘Šã€—ã€¦ã€„ã€Ÿã€ ã€„ã€ŸBBVAã€®Guillermo Muñoz Mozosæ°€ã€«æ„Ÿè¬ã€„ã€Ÿã€—ã€¾ã€™ã€,

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes

æ”¹è¨‚å±¥æ´

ãƒ•ã‚¡ã‚¤ãƒ«ã‚¿ã‚¤ãƒ—	èª¬æ˜Ž	
1.2	FTDã•®ä¿®æ£æ¸ˆã•¿ãƒªãƒªãƒ¼ã‚¹æ…å ±ã‚’æ›´æ–°ã€‚	ä¿®æ£æ¸ˆã•¿ã‚½ãƒ•ã
1.1	FTDã•Šã‚ˆã•³Snort 3ã•®æƒ…å ±ã‚’è¿½åŠ ã€‚Catalystè£½å“•ã‚’è¿½åŠ ã€‚Cisco FTDãƒªãƒªãƒ¼ã‚¹6.7.0ã•®å›žé•ç–ã‚’è¿½åŠ ã€‚	æ¦‚è¦•ã€•è„†å¼±æ€
1.0	åˆ•å›žå…¬é–‹ãƒªãƒªãƒ¼ã‚¹	-

åˆ©ç”¨è¦•ä»¶

æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã•¯ã€„ä¿¡é ¼ã•§ã••ã•®ã•¨ã•—ã•¦ã•”æ••ä¾›ã•—ã•¦ã•Šã€
æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã•®æƒ…å ±ã•Šã‚ˆã•³ãƒªãƒªãƒ¼ã‚¯ã•®ä½¿ç”¨ã«é–¢ã•™ã‚‹è²¬ä»»ã•¯ã€
ã•¾ã•Ÿã€•ã‚·ã‚¹ã‚³ã•¯æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã•®å†…å®¹ã‚’äº‹å‰Šã•ªã•—ã•«å¤‰æ›´ã•—ã•
æœ¬ã‚¢ãƒ‰ãƒã‚¤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,¶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。