Ciscoé©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã, Firepower Threat Defenseã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®AnyConnect SSL VPNã«ãŠã‘ã‚‹DoSè„†å¼±æ€§

Medium

ã,¢ãƒ‰ãƒ©ã,¤ã,¶ãƒªãƒ¼ID : cisco-sa-vpndtls-dos-TunzLEV

CVE-2022-20795

å^©å...¬é–‹æ—¥ : 2022-04-20 16:00

æœ€çµ‚æ›´æ–°æ—¥ : 2022-05-02 17:17

ãƒãƒ¼ã,¸ãƒ§ãƒ³ 1.1 : Final

CVSSã,¹ã,³ã,¢ : 5.8

å›žé¿ç– : No workarounds available

Cisco ãƒã,° ID : CSCvz09106

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

æ¦‚è¦

Ciscoé©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹(ASA)ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€Šã,ˆã€³Cisco Firepower Threat Defense(FTD)ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã«ã€Šã€‘ã,‹ãƒ‡ãƒ¼ã,¿ã,°ãƒ©ãƒ TLS(DTLS)ãƒ—ãƒãƒˆã,³ãƒ«ã€®å®Ÿè

ã€“ã€®è„†å¼±æ€§ã€¯ã€AnyConnect SSL VPNæŽ¥ç¶šã®ä¸€éƒ¨ã¨ã—ã¦DTLSãƒˆãƒ³ãƒãƒ«ã,’ç¢ºç«‹ã™ã,‹éš›ã«ç™ºç”Ÿã™ã,‹æœ€é

æ³¨ï¼šæ”»æ’ƒãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ã€Œå¤œæ¢ã™ã,‹ã¨ã€ãƒ‡ãƒã,¤ã,¹ã€¯æ£å¸¸ã«å›žå¾©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‰ãƒã,¤ã,¶ãƒªã€¯æ¬¡ã€®ãƒªãƒ³ã,¯ã,ˆã,Šç¢ºèªã§ã••ã¾ã™ã€‚
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vpndtls-dos-TunzLEV

è©²å½“è£½å“

è„†å¼±æ€§ã®ã,ã‚‹è£½å“

ã€“ã€®è„†å¼±æ€§ã¯ã€Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã¾ãŸã¯Cisco FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®è„†å¼±æ€§ã€Œå˜ä¸€ã™ã,‹ãƒªãƒªãƒ¼ã,¹ã,’å®Ÿè¡Œã—ã€AnyCon

SSL
VPNæŽ¥ç¶šã®DTLSãƒˆãƒ³ãƒãƒ«ã‚’çµ‚äº†ã™ã‚‹ã‚ˆã†ã«è¨å®šã•ã‚Œã¦ã„ãªã„ã‹ã‚’

è„†å¼±æ€§ã€Œå˜åœ¨ã™ã‚‹ Cisco
ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ã‚’å®Ÿè¡Œã—ã¦ã„ã‚‹ã‚¢ãƒ€ãƒ—ãƒ†ãƒƒãƒ‰ã‚¤ãƒ³ã‚¹ã‚¿ãƒ³ã‚¹ã®
ID ã€®è©³ç´°ã‚»ã‚¯ã‚·ãƒ§ãƒ³ã‚’å€‚ç…§ã—ã¦ãã ã•ã„ã€‚

**æ³¨ï¼šSSL VPNã€¯ãƒ‡ãƒ•ã‚©ãƒ«ãƒˆã§§ç„¡åŠ¹ã«ã€ªã£ã¦ã„ã¾ã™ã€‚SSL
VPNã€Œã‚¤ãƒ³ã‚¿ãƒ¼ãƒ•ã‚§ãƒ¼ã‚¹ã€§æœ‰åŠ¹ã«ã€ªã£ã¦ã„ã‚‹å ´å^ˆã€DTLSã€¯ãƒ‡ãƒ

ãƒ‡ãƒ•ã‚©ãƒ«ãƒˆè¨å®šã®ç¢ºèª

AnyConnect SSL
VPNã€ŒDTLSæŽ¥ç¶šã«å¯¾ã—ã¦æœ‰åŠ¹ã§§è¨å®šã•ã‚Œã¦ã„ã‚‹å ´å^ˆã€ã‚¯ãƒ©ã‚¤ã‚¢ãƒ³ãƒˆã€
asp table socket | include DTLSã‚³ãƒžãƒ³ãƒ‰ã‚’ä½¿ç”¨ã—ã¦ã€ã¾ã™ã€‚

ã€“ã®æ©Ÿèƒ½ã€Œè¨å®šã•ã‚Œã¦ã„ãªã„å ´å^ˆã€ã€“ã®ã‚³ãƒžãƒ³ãƒ‰ã¯å‡ºåŠ›

<#root>

device#

show asp table socket | include DTLS
DTLS 00056858 LISTEN 192.168.1.6:443 0.0.0.0:*

æ³¨ï¼šCisco
FTDã‚½ãƒ•ãƒˆã‚¦ã‚§ãƒ¢ãƒ¼ãƒ‰ã€¯ã€»ã‚¹VPNæ©Ÿèƒ½ã€¯ãƒªãƒªãƒ¼ã‚¹6.2.2ã€‹ã‚‰ã‚µãƒ¼ã

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

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

ã‚·ã‚¹ãƒ†ãƒ ã€¯ã€“ã®è„†å¼±æ€§ã€Œ Cisco Firepower Management
Centerï¼ˆFMCï¼‰ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ã€«å½±éŸ¿ã‚’å€Šã¼ã•ã€ªã„ã“ã¨ã‚’ç¢ºèªã—ã—ã—

ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£å¾Œ®³ã€®ç—•è·¡

ã€“ã®è„†å¼±æ€§ã€Œä¸€æ£åˆ©ç”¨ã•ã‚Œã‚‹ã¨ã¨ã€¯ã€€è©²å½“ã™ã‚‹ãƒ‡ãƒã‚¤ã‚¹ã‚¿ã§§ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
asp drop | include np-socket-new-conn-failureã€Šã‚ˆã€³**show counters | include
HANDLE_ALLOC_FAILED** ã‚³ãƒžãƒ³ãƒ‰ã‚’æ¬¡ã€«ç¤ºã—ã€—ã¾ã™ã€‚

<#root>

```
device#
show asp drop | include np-socket-new-conn-failure
Flow drop:
NP socket new connection failure (np-socket-new-conn-failure) 160299

device#
show counters | include HANDLE_ALLOC_FAILED
CRYPTO      HANDLE_ALLOC_FAILED                                 160339
```

ã€“ã,Œã,‰ã®ã,«ã,¦ãƒ³ã,¿å€¤ã€Œé•·æœŸé–“æ€¥é€Ÿã«å¢—åŠ ã™ã,‹å ´å•ˆã¯ã€Cisco Technical Assistance Center(TAC)ã«é€£çµ¡ã—ã¦ã€è©³ç´°ã•èª¿æŸ»ã,’ä¾é ¼ã—ã¦ãã ã•ã„ã€,

å›žé¿ç–

ã“ã®è„†å¼±æ€§ã«å¯¾å‡¦ã™ã,‹å›žé¿ç–¯ã¯ã,Šã¾ã›ã,“ã€,ã€Ÿã• ã—ã€ç®¡ç
<interface> tls-onlyã,³ãƒžãƒ³ãƒ‰ã,’使ç”¨ã—ã¦ã—ã¦ã„ã,‹å ´å•ˆã¯ã€ç·©å’Œç–¯ã¨ã—ã¦SSL DTLS VPNæŽ¥ç¶šã,’ç„¡åŠ¹ã«ã™ã,‹ã“ã¨ã€æ¬¡ã®ä¾‹ã,’ã”è¦§ãã

```
<#root>
device(config-webvpn)#
enable outside tls-only
```

**æ³¨ï¼šDTLSã,’ç„¡åŠ¹ã«ã™ã,‹ã¨ã€VPNã®ãƒãƒ•ã,©ãƒ¼ãƒžãƒ³ã,¹ã€Œå¤§å¹…ã«ä½Žä¸‹ã™ã

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

代æ£æ¸ˆã¿ã•ãƒˆã,¦ã,§ã,¢

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,’検討ã™ã,‹éš›ã«ã¯ã€ã,·ã,¹ã,³ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ‰ãƒ—ã,¤ã,¶ãƒªã,’å®šæœŸçš„ã«å¸‚,ã,½ãƒªãƒ¥ãƒ¼ã,·ãƒ§ãƒ³ä¸€è¼ã,’ç¢ºèªã—ã¦ã—ã¦ã„ã,‹ã,·ã,¹ã,³è£½å“ã®ã,¢ãƒ‰ãƒ

ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹

ç™ºè¡Œæ™‚ç‚¹ã€§ã€¯ã€€æ¬¡ã€®è¨¨ã€®ãƒªãƒªãƒ¼ã‚¹ãŒæ…å ±ã€¯æ£ç°ã€§ã€—ã€Ÿã€‚æœ€æ–°

å·¦ã€®åˆ—ã€¯ã€·ã‚¹ã‚³ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ã‚’ç¤ºã€—ã€€å€³ã€®åˆ—ã€¯ãƒªãƒªãƒ¼ã‚¹ã€

ASA ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢

Cisco ASA ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ ãƒªãƒªãƒ¼ã‚¹	ã€“ã€®è„†å¼±æ€§ã€«å¯¾ã€™ã‚‹æœ€åˆ€ã€®ä¿®æ£ãƒªãƒªãƒ¼ã‚¹
9.7 ä»¥å‰ [1]	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œ
9.8	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,
9.91	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,
9.101	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,
9.12	9.12.4.41ï¼ˆ2022å¹´6月ï¼‰
9.131	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,
9.14	9.14.4.8ï¼ˆ2022å¹´6月ï¼‰
9.15	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œ
9.16	9.16.3.3
9.17	9.17.1.10ï¼ˆ2022å¹´6月ï¼‰

1. Cisco ASA ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ 9.7 ä»¥å‰ã€€ã€Šã‚ˆã³ 9.9ã€€9.10ã€€9.13 ãƒªãƒªãƒ¼ã‚¹ã€§ã€¤ã€„ã€¦ã€¯ã€€
ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã®ã¿ãªã‚“ãƒ†ãƒŠãƒ³ã‚¹ã€Œçµ‚äº†ã€—ã€¦ã€„ã€¾ã€™ã€‚ã€“ã€®è„†å¼±æ€§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
6.2.2 [1]	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,
6.2.3	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,
6.3.0 [1]	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,
6.4.0	6.4.0.15 (May 2022)
6.5.01	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,
6.6.0	6.6.7ï¼ˆ2022å¹´6月ï¼‰
6.7.0	ä¿®æ£æ¸ˆã€¿ãƒªãƒªãƒ¼ã‚¹ã€§ç§»è¡Œã€,

Cisco FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã,¹	ã"ã®è„†å¼±æ€§ã«å¯¾ã™ã‚‹æœ€å^ã®ä¿®æ£ãƒªãƒªãƒ¼ã,¹
7.0.0	7.0.2 (May 2022)
7.1.0	7.1.0.3ï¼ˆ2022å¹´10月ï¼‰

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€œ6.5.0 ã«ã¤ã„ã¦ã¯ã€

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹ã€Œçµ,äº†ã—ã¦ã„ã„ã¾ã™ã€‚ã"ã®è„†å¼±æ€§ã

ä¸€æ£å^©ç"¨äº‹ä¾‹ã¨å…¬å¼€ç™ºè¡¨

Cisco Product Security Incident Response Teamï¼^PSIRTï¼‰ã¯ã€ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªãƒ¼§èª¬æ˜Žã•ã,Œã¦ã„ã„ã,‹è„†å¼±æ€§ã«å¯¾ã,³ãƒ¼ãƒ‰ã€Œå…¥æ‰‹å¯¯èƒ½ã§ã,‹ã"ã¨ã,'èª¯è˜ã—ã¦ã„ã„ã¾ã™ã€,

ã"ã®ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªãƒ¼§èª¬æ˜Žã•ã,Œã¦ã„ã„ã,‹è„†å¼±æ€§ã®æ,ªç"¨ã«é–¢ã™ã,‹æ
Cisco PSIRT ã«å¯„ã›ã‚‰ã,Œã¦ã„ã„ã¾ã›ã,"ã€,

å‡ºå…¸

ã"ã®è„†å¼±æ€§ã,'å ±å'Šã—ã¦ã„ã„ãŸã ã„ãŸYETH Zurichã®Fabio Streunæ°ã«æ„Ÿè¬ã„ãŸã„ãŸã—ã¾ã™ã€,

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vpndtls-dos-TunzLEV

æ”¹è¨,å±¥æ´

ãƒãƒ¼ã,¸ãƒ§ãƒ³	èª¬æ˜Ž	
1.1	è©²å½"ãƒªãƒªãƒ¼ã,¹ã«¨ä¿®æ£æ¸ˆã•ãƒªãƒªãƒ¼ã,¹ã®æƒ…å ±ã,'è¿½åŠ ã€,	ã€Œè„†
1.0	å^•å›žå…¬é–‹ãƒªãƒªãƒ¼ã,¹	-

å^©ç"¨è¦ç´„

æœ¬ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªãƒ¯ã¯ã®ã,,ã®ã¨ã¨ã—ã¦ã—ã¦ã"æ••ä¾›ã—ã¦ã„ã‚‹ã€Šã
æœ¬ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªãƒ¯ã®æƒ…å ±ã‚ˆã³ãƒªãƒ³ã,¯ã®ä½¿ç"¨ã«é–¢ã™ã,‹è²¬ä»»ã®ä¸€
ã¾ãŸã€·ã,¹ã,³ã¯æœ¬ãƒ‰ãƒ¡ãƒ³ãƒˆã®å†…å®¹ã,'ä°^å'Šã¯ã—ã«å¤‰æ›´ã—ã
æœ¬ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªãƒ¯ã®è¨˜è¿°å†…å®¹ã«é–¢ã—ã¦æƒ…å ±é…ä¿¡ã® URL

ã,'çœ•¥ã—ã€å˜ç‹¬ã®è»¢è¼‰ã„„æ„è¨³ã,'æ–½ã—ã Ÿå´å^€å½“¤¾ãŒç®¡ç
ã“ã®ãƒ‰ã,ãƒ¥ãƒ¡ãƒ³ãƒˆã®æƒ…å ±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。