è¤‡æ•°ã�®ã,·ã,¹ã,³è£½å“�ã�«ã�Šã�‘ã,‹Snort
HTTPæ¤œå‡ºã,¨ãƒ³ã,¸ãƒ³ã�®ãƒ•ã,¡ã,¤ãƒ«ãƒ�ã,

Medium

ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªãƒ¼ID : cisco-sa-snort-filepolbypass-67DEwMe2

å^�å…¬é–‹æ—¥ : 2021-01-13 16:00

æœ€çµæ›´æ–°æ—¥ : 2021-04-30 16:09

ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ 1.1 : Final

CVSSã,¹ã,³ã,¢ : 5.8

å›žé�¿ç– : No workarounds available

Cisco ãƒ�ã,° ID : CSCvs71969 CSCvu18635

CVE-2021-1223

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�Œã€�Snortæ¤œå‡ºã,¨ãƒ³ã,¸ãƒ³ã�®è„†å¼±æ€§ã�®å½±éŸ¿ã,’å�—ã�

ã�“ã�®è„†å¼±æ€§ã�¯ã€�HTTPç¯„å›²ãƒ˜ãƒƒãƒ€ãƒ¼ã�®ä¸�é�©åˆ‡ã�ªå‡¦ç�†ã�«èµ·å› 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�¯ã€�æ¬¡ã�®ãƒªãƒ³ã,¯ã,ˆã,Šç¢ºèª�ã�§ã��ã�¾ã�™ã€,
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2

è©²å½“è£½å“�

è„†å¼±æ€§ã�®ã�,ã,‹è£½å“�

å…¬é–‹æ™‚ç‚¹ã�§ã�¯ã€�ã�“ã�®è„†å¼±æ€§ã�¯ãƒªãƒªãƒ¼ã,¹2.9.17ã,ˆã,Šå‰�ã�®ã�™ã�¹ã�
ã�® Web ã,µã,¤ãƒˆã,’å�‚ç…§ã�—ã�¦ã��ã� ã�•ã�„ã€,

ã�“ã�®è„†å¼±æ€§ã�®å…¬é–‹æ™‚ç‚¹ã�§ã€�ã,·ã,¹ã,³ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®è„†å¼±æ€§ã�Œå

- 3000 ã,·ãƒªãƒ¼ã,ºç”£æ¥ç”¨ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ï¼ˆISAï¼‰
- Firepower Threat Defenseï¼ˆFTDï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

å…¬é–‹æ™‚ç‚¹ã�§ã€�ã�“ã�®è„†å¼±æ€§ã�¯ã€�Cisco IOS XEã,½ãƒ•ãƒˆã,¦ã,§ã,¢ç”¨ã�®Cisco Unified Threat Defense(UTD)Snort Intrusion Protection

System(IPS)ã‚¨ãƒ³ã‚¸ãƒ³ã€�ã�¾ã�Ÿã�¯Cisco IOS XE SD-WANã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ç”¨ã�®Cisco UTDã‚¨ãƒ³ã‚¸ãƒ³ã�®æœ€åˆ�ã�®ä¿®æ£æ¸ˆã�¿ãƒªãƒªãƒ¼ã‚¹ã‚ˆã‚Šã‚‚å‰�ã�®ãƒªãƒªãƒ¼ã‚¹ã‚’å®

- 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‰
- Cloud Services Router 1000V
- ã‚µãƒ¼ãƒ“ã‚¹çµ±å�ˆåž‹ä»®æƒ³ãƒ«ãƒ¼ã‚¿ï¼ˆISRvï¼‰

å…¬é–‹æ™‚ç‚¹ã�§è„†å¼±æ€§ã�Œç¢ºèª�ã�•ã‚Œã�¦ã�„ã‚‹ Cisco ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã�®ãƒªãƒªãƒ¼ã‚¹ã�«ã�¤ã�„ã�¦ã�¯ã€�ã�“ã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã�® ID ã�®è©³ç´°ã‚»ã‚¯ã‚·ãƒ§ãƒ³ã‚’å�‚ç…§ã�—ã�¦ã��ã� ã�•ã�„ã€‚

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‚¢
- Firepower Management Centerï¼ˆFMCï¼‰ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢
- 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�¯ã�‚ã‚Šã�¾ã�›ã‚“ã€‚

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‰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��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€�Cisco Firepower Threat Defense(FTD)ãƒªãƒªãƒ¼ã‚¹6.7.0ä»¥é™�ã�«ã�“ã�®è„†å¼±æ€§ã�«å¯¾ã�™ã‚‹ä¿®æ£ã�Œå�«ã�

å…¬é–‹æ™‚ç‚¹ã�§ã�¯ã€�Cisco UTD Snort IPS Engine Software for IOS XE 17.4.1[1]ã�«ã�“ã�®è„†å¼±æ€§ã�«å¯¾ã�™ã‚‹ä¿®æ£ã�Œå�«ã�¾ã‚Œã�¦ã�„ã�¾ã�™ã€‚

å…¬é–‹æ™‚ç‚¹ã�§ã�¯ã€�ã‚ªãƒ¼ãƒ—ãƒ³ã‚½ãƒ¼ã‚¹ã�®Snortãƒ—ãƒã‚¸ã‚§ã‚¯ãƒˆã�®ãƒªãƒªãƒ¼ã‚¹2.9.17 ã�® Web ã‚µã‚¤ãƒˆã‚’å�‚ç…§ã�—ã�¦ã��ã� ã�•ã�„ã€‚

æœ€ã‚‚å®Œå…¨ã�§æœ€æ–°ã�®æƒ…å ±ã�«ã�¤ã�„ã�¦ã�¯ã€�ã�“ã�®ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªã� ID ã�®è©³ç´°ã‚»ã‚¯ã‚·ãƒ§ãƒ³ã‚’å�‚ç…§ã�—ã�¦ã��ã� ã�•ã�„ã€‚

1. 17.2.1ä»¥é™�ã�§ã�¯ã€�IOS XEã�¨IOS 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‰ãƒ�ã‚¤ã‚¶ãƒªã�«è¨˜è¼‰ã�•ã‚Œã�¦ã�„ã‚‹è„†å¼±æ€§ã�

å‡ºå…¸

ã�“ã�®è„†å¼±æ€§ã�¯ ã€�ã‚·ã‚¹ã‚³å†…éƒ¨ã�§ã�®ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ãƒ†ã‚¹ãƒˆä¸ã�« Ilkin Gasimov ã�«ã‚ˆã�£ã�¦ç™ºè¦‹ã�•ã‚Œã�¾ã�—ã�Ÿã€‚

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2

æ”¹è¨‚å±¥æ´

ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³	èª¬æ˜Ž	ã‚»ã‚¯ã‚·ãƒ§ãƒ³
1.1	Unified Threat Defenseã�®ãƒªãƒªãƒ¼ã‚¹æƒ…å ±ã‚’è¿½åŠ ã€‚	è„†å¼±æ€§ã�Œå˜åœ¨ã�™ã‚‹è£½å“
1.0	åˆ�å›žå…¬é–‹ãƒªãƒªãƒ¼ã‚¹	-

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