Cisco Advanced Malware Protection for Endpointsã�®Windowsã,³ãƒžãƒ³ãƒ‰ã,¤ãƒ³ã,¸ã,

Medium

ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªãƒ¼ID : cisco-sa-20190703-amp-commandinj

[CVE-2019-1932](CVE-2019-1932)

åˆ�å…¬é–‹æ—¥ : 2019-07-03 16:00

ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ 1.0 : Final

CVSSã,¹ã,³ã,¢ : 6.7

å›žé�¿ç– : No workarounds available

Cisco ãƒ�ã,° ID : CSCvp53361

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

æ¦‚è¦�

Windowsç”¨ã,¨ãƒ³ãƒ‰ãƒ�ã,¤ãƒ³ãƒˆå�‘ã�‘Cisco Advanced Malware Protection(AMP)ã�®è„†å¼±æ€§ã�«ã,ˆã,Šã€�ç®¡ç�†è€…æ¨©é™�ã,’æŒ�ã�¤èª�è¨¼ã�•ã,Œã�

ã�“ã�®è„†å¼±æ€§ã�¯ã€�å‹•çš„ã�«ãƒãƒ¼ãƒ‰ã�•ã,Œã,‹ãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«ã�®æ¤œè¨¼ã�Œä¸�å

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-20190703-amp-commandinj

è©²å½“è£½å“�

ã�“ã�®ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�«è¨˜è¼‰ã�•ã,Œã�¦ã�„ã,‹æƒ…å ±ã�¯ã€�ç™ºè¡Œæ™,ç,¹ã�§å…

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,’æ¤œè¨Žã�™ã,‹éš›ã�«ã�¯ã€�[ã,·ã,¹ã,³ã�®ã,»ã,ãƒ Security Advisories and Alertsï¼‰] 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§ãƒ³ã,’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

è¿½åŠ æƒ…å ±ã�Œå¿…è¦�ã�ªå ´å�ˆã�¯ã€�Cisco Technical Assistance Center(TAC)ã�¾ã�Ÿã�¯å¥‘ç´„ã�—ã�Ÿãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹ãƒ—ãƒãƒ�ã,¤ãƒ€ãƒ¼ã�«é€£çµ¡ã�™ã,‹ã

è„†å¼±æ€§ã�®ã�‚ã‚‹è£½å“�

å…¬é–‹æ™‚ç‚¹ã�§ã�¯ã€�ã�“ã�®è„†å¼±æ€§ã�¯Windowsãƒªãƒªãƒ¼ã‚¹6.2.3.10807_030519ä»¥å
AMP for Endpointsã�«å½±éŸ¿ã‚’ä¸Žã�ˆã�¾ã�—ã�Ÿã€‚

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�

- ã‚¨ãƒ³ãƒ‰ãƒ�ã‚¤ãƒ³ãƒˆå�‘ã�‘ AMP for Mac
- ã‚¨ãƒ³ãƒ‰ãƒ�ã‚¤ãƒ³ãƒˆå�‘ã�‘ AMP for Linux

ä¿®æ£æ¸ˆã�¿ãƒªãƒªãƒ¼ã‚¹

å…¬é–‹æ™‚ç‚¹ã�§ã�¯ã€�Cisco AMP for Endpoints for Windowsãƒªãƒªãƒ¼ã‚¹6.3.3ä»¥é™�ã�«ã�“ã�®è„†å¼±æ€§ã�«å¯¾ã�™ã‚‹ä¿®æ£ã�Œå�«ã�¾

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£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‚¹ã‚³ã�¯ã€�ã�“ã�®è„†å¼±æ€§ã‚’å ±å‘Šã�—ã�¦ã�„ã�Ÿã� ã�„ã�ŸNSS Labsã�®Edsel Valleæ°�ã�«æ„Ÿè¬�ã�„ã�Ÿã�—ã�¾ã�™ã€‚

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-amp-commandinj

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	2019 å¹´ 7 æœˆ 3 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