ã,·ã,¹ã,³è£½å“ã«å½±éŸ¿ã™ã,‹TLSã«å¯¾ã

Medium

ã,¢ãƒ‰ãƒ¤ã,¤ã,¶ãƒªãƒ¼ID : cisco-sa-20171212-bleichenbacher

å^å...¬é–‹æ—¥ : 2017-12-12 15:45

æœ€çµ‚æ›´æ–°æ—¥ : 2018-05-18 17:31

ãƒãƒ¼ã,¸ãƒ§ãƒ³ 1.6 : Final

CVSSã,¹ã,³ã,¢ : 5.3

å›žé¿ç– : Yes

Cisco ãƒã,° ID : CSCvh00296 CSCvg74693 CSCvg97652 CSCvh10981 CSCvh25064

CVE-2017-15533
CVE-2017-12373
CVE-2017-17428

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

æ¦‚è¦

2017å¹´12æœˆ12æ—¥ã€ *Return of Bleichenbacher's Oracle Threat*ã¨ã„ã†ã,¿ã,¤ãƒˆãƒ«ã®ç ”ç©¶è«–æ–‡ãŒå...¬é–‹ã•ã,Œã¾ã—ãŸã€‚ã“ã®ãƒ¬ Layer Security(TLS)ã,¹ã,¿ãƒƒã,¯ã€Œã€RSAã,ãƒ¼äº¤æ›ã«å¯¾ã™ã,‹å¾“æ¥ã®Bleichenbacheræ”»

æ”»æ’ƒè€…ã¯ã€è„†å¼±ã²TLSã,¹ã,¿ãƒƒã,¯å®Ÿè£…ã,’å®Ÿè¡Œã—ã¦ã„ã,µãƒ¼ãƒ–ã«å¯¾

ã“ã,Œã,‰ã®è„†å¼±æ€§ã,’ä¸Žæ£å^©ç”¨ã™ã,‹ã«ã¯ã¯ã€æ”»æ’ƒè€…ã¯æ¬¡ã®ä¸æ–¹

- ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆå½±éŸ¿ã,’å—ã‘ã,‹TLSã,µãƒ¼ãƒ–é–“ã®ãƒˆãƒ©ãƒ•ã,£ãƒƒã,¯ã,’ã,ãƒ£ãƒ—
- è„†å¼±ã²ã,µãƒ¼ãƒ–ã¸ã®TLSæŽ¥ç¶šã,’ç©•æ¥µçš„ã«ç¢ºç«‹ã—ã¾ã™ã€‚å®Ÿéš›ã

è¤‡æ•°ã®ã,·ã,¹ã,³è£½å“ã«ã,Œã€ã“ã,Œã,‰ã®è„†å¼±æ€§ã®å½±éŸ¿ã,’å—ã‘ã¾ã™ã

ã,·ã,¹ã,³ã¯ã€ã“ã,Œã,‰ã®è„†å¼±æ€§ã®ä¸€éƒ¨ã«å¯¾å‡¦ã™ã,‹ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,¢ãƒƒã

é¸æŠžã—ã—ãŸè£½å“ã«å¯¾ã—ã¦å›žé¿ç–ã€ã,ã,‹å¯¯èƒ½æ€§ã€ã,Šã¾ã™ã

ã�“ã�®ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�¯ã€�æ¬¡ã�®ãƒªãƒ³ã,¯ã,ˆã,Šç¢ºèª�ã�§ã��ã��ã¾ã�™ã€,
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171212-bleichenbacher

è©²å½“è£½å“�

ã,·ã,¹ã,³ã�§ã�¯ã€�æœ¬è„†å¼±æ€§ã�®å½±éŸ¿ã,’å�—ã�‘ã,‹è£½å“�ã��ä½±éŸ¿ã�®ç¯„å›²ã,’ç‰¹

ã€Œè„†å¼±æ€§ã�Œå˜åœ¨ã�™ã,‹è£½å“�ã€�ã,»ã,¯ã,·ãƒ§ãƒ³ã�«ã�¯ã€�å½±éŸ¿ã,’å�—ã�‘ã,‹å�„è
Bug IDã�Œè¨˜è¼‰ã�•ã,Œã�¦ã�„ã�¾ã�™ã€,Cisco Bug ã�¯ Cisco Bug Search Tool
ã�§æ¤œç´¢å¯¯è±¡ã,ã,Šã€�å›žé¿ç–¼ï¼ˆä½¿ç”¨å¯¯è±¡ãªå ´å�ˆï¼‰ã��ä¿®æ£ã�•ã,Œã
ãƒªãƒªãƒ¼ã,¹ã�ªã�©ã€�ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ å›ºæœ‰ã�®è¿½åŠ æ…‹å ±ã�Œè¨˜è¼‰ã�•ã

è„†å¼±æ€§ã�®ã�,ã,‹è£½å“�

æ¬¡ã�®è¡¨ã�«ã€�ã“ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�«è¨˜è¼‰ã�•ã,Œã�Ÿ 1
ã�¤ä»¥ä¸Šã�®è„†å¼±æ€§ã�®å½±éŸ¿ã,’å�—ã�‘ã,‹ã,·ã,¹ã,³è£½å“�ã,’ç¤ºã�—ã�¾ã�™ã€,

è£½å“�	Cisco Bug ID	
ã,·ã,¹ã,³ ã,¯ãƒ©ã,¦ãƒ‰ ãƒ›ã,¹ãƒ†ã		
Cisco WebEx Business Suiteï¼ˆMeeting Centerã€�Training Centerã€�Event Centerã€�Support Centerã€ªã€©ï¼‰	CSCvh10981	ä¿®å¾©æ¸ˆã€
Cisco WebEx Meetings	CSCvh10981	ä¿®å¾©æ¸ˆã€
Cisco WebEx Messenger	CSCvh25064	ä¿®å¾©æ¸ˆã€
ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã,¯ ã,¢ãƒ—ãƒªã,±ãƒ¼ã,·ãƒ§ãƒ³ã€ã,µãƒ¼ãƒ		
Cisco ACE 4710 Application Control Engineã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹	CSCvg74693	ã€“ã€®è£½å“
Cisco ACE30 Application Control Engineãƒ¢ã,¸ãƒ¥ãƒ¼ãƒ«	CSCvg74693	ã€“ã€®è£½å“
ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã,¯ã€Šã,ˆã€³ã,³ãƒ³ãƒ†ãƒ³ãƒ		
Ciscoé€©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹(ASA):ASA 5505ã€�5510ã€�5520ã€�5540ã€ã€Šã,ˆã€³5550	CSCvg97652	9.1.7.21ï¼ˆ2018å¹´ 9.2.4.25ï¼ˆ2018å¹´
Cisco SSLã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹	CSCvh00296	3.12.2.1ï¼ˆ2018å¹´

[1] Cisco ACE 4710 Application Control
Engineã‚¢ãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹ã€2013å¹´7月26æ—¥ã«ãƒ©ã‚¤ãƒ•ã‚µã‚¤ã‚¯ãƒ«çµ‚了ã‚’è¿Žã€
è²©å£²çµ‚了ã€ã‚µãƒãƒ¼ãƒˆçµ‚了ã®ãŠçŸ¥ã‚‰ã›ã€‚ã‚’å‚ç…§ã—ã¦ãã ã

[2] Cisco ACE30 Application Control
Engineãƒ¢ã‚¸ãƒ¥ãƒ¼ãƒ«ã€2013å¹´7月26æ—¥ã«ãƒ©ã‚¤ãƒ•ã‚µã‚¤ã‚¯ãƒ«çµ‚了ã‚’è¿Žã€
è²©å£²çµ‚了ã€ã‚µãƒãƒ¼ãƒˆçµ‚了ã®ãŠçŸ¥ã‚‰ã›ã€‚ã‚’å‚ç…§ã—ã¦ãã ã

è„†å¼±æ€§ã‚’å«ã‚“ã§ã„ãªã„ã“ã¨ãŒç¢ºèªã•ã‚Œã¦ã„ã‚‹è£½å“

ä»–ã®ã‚·ã‚¹ãƒ†ãƒ ã¸ã®è£½å“ã«ã‚‚ã„ã¦ã‚‚ã€ãƒ‘ãƒƒãƒã‚¢ãƒƒãƒ—ã‚’å—ã‘ã‚‹ã“ã‚‚ã‚ã‚Šã€

ã‚·ã‚¹ãƒ†ãƒ ã¯ã€Œè„†å¼±æ€§ã‚Œä»¥ä¸‹ã®è£½å“ã«ã¯å½±éŸ¿ã‚’ä¸Žã‚ˆã

ã‚·ã‚¹ãƒ†ãƒ ã‚¯ãƒ©ã‚¦ãƒ‰ ãƒ›ã‚¹ãƒ†ãƒƒãƒ‰ ã‚µãƒ¼ãƒ“ã‚¹

- Cisco Cloud Web Security(CWS)
- Cisco Spark
- Cisco Umbrella

ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã‚¯
ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³ã€µãƒ¼ãƒ“ã‚¹ã€ãŠã‚ˆã³ã‚³ãƒ³ãƒ†ãƒ³ãƒ„ ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£

- Cisco Wide Area Application Servicesï¼ˆWAASï¼‰

ãƒ•ãƒƒãƒˆãƒ¯ãƒ¼ã‚¯ã€ãŠã‚ˆã³ã‚³ãƒ³ãƒ†ãƒ³ãƒ„ ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ ãƒ‡ãƒã‚¤ã‚¹

- Ciscoé©©å¿œåž‹ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ã‚¢ãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹(ASA):ã€Œè„†å¼±æ€§ã®ã‚ã‚‹è£½
- Cisco ASA Next-Generation Firewall Services
- Cisco Content Security Management Appliance (SMA)
- Cisco Email Security Appliance (ESA)
- Cisco Firepower 2100 ã‚·ãƒªãƒ¼ã‚º
- Cisco Firepower 4100 ã‚·ãƒªãƒ¼ã‚º
- Cisco Firepower 7000 ã‚·ãƒªãƒ¼ã‚º
- Cisco Firepower 8000 ã‚·ãƒªãƒ¼ã‚º
- Cisco Firepower 9300ã‚·ãƒªãƒ¼ã‚ºã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³
- Cisco Identity Services Engineï¼ˆISEï¼‰

- Cisco Web Security Appliance (WSA)

Routing and Switching - Enterprise and Service Provider

- Cisco VPN Internal Service Module for ISR(VPN ISM)

è©³ç´°

Bleichenbacherã®æ”»æ’ƒã¯ã€RSA PKCS#1
v1.5æš—å·åŒ–ãƒ–ãƒƒãƒ‰ã¯ãƒ•ã‚©ãƒžãƒƒãƒˆã«å¯¾ã™ã‚‹é©©å¿œåž‹é¸æŠžæš—å·æ–‡(cho
ciphertext)æ”»æ’ƒã§ã™ã€‚Daniel Bleichenbacherã¯å½“å^ã€Secure Sockets
Layer(SSL)ãƒãƒ¼ã‚¸ãƒ§ãƒ³3.0ã§RSAã‚ãƒ¼äº¤æ›ã«å¯¾ã—ã¦æ”»æ’ƒã‚’å®Ÿè¡Œã—

ã“ã®æ”»æ’ƒã¯ã€é¸æŠžã•ã‚Œã‚Ÿæš—å·æ–‡ã«ã¤ã„ã¦ã€å¯¾å¿œã™ã‚‹13æ
PKCS#1
v1.5æ¨™æº–ã«å¾“ã£ã¦æ£ã—ã„å½¢å¼ã«ã‚‰ã‚Œã¦ã„ã‚‹ã‹ã‚’ç¤ºã™ã‚‚ã‚µãƒ‰ãƒ£ãƒ

ã“ã®æ–°ã—ã„ ”ç©¶ã§ã¯ã€å¾“æ¥ã®Bleichenbacheræ”»æ’ƒã®å½±éŸ¿ã‚’å—ã‘ã

ã“ã®èª¿æŸ»ã«åŸºã¥ã„ã¦ã¦ã¯æ¬¡ã®è„†å¼±æ€§ã‚Œç‰¹å®šã•ã‚Œã¾ã—ãŸã

Cavium SSL SDK Bleichenbacheræ”»æ’fæf…å ±æ¼ãã^ã„ã®è„†å¼±æ€§

Cavium
SSLã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢é–‹ç™ºã‚ãƒƒãƒˆ(SDK)ã®TLSãƒ—ãƒƒãƒˆã‚³ãƒ«å®Ÿè£…ã«ã«ãŠã‘ã‚‹è„†å¼±æ€§ã

ã“ã®è„†å¼±æ€§ã¯ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã«RSAã‚’ä½¿ç”¨ã™ã‚‹æš—å·ã‚¹ãƒ¼ãƒˆã«å¯¾ã

ã“ã®è„†å¼±æ€§ã¯CVE IDã¨ã—ã¦CVE-2017-
17428ã€Œå‰²ã‚Šå½“ã¦ã¦ã„ã‚‰ã‚Œã¦ã„ã¾ã™ã€‚

**ãƒ¬ã‚¬ã‚·ãƼCisco ASA
5500ã‚·ãƒªãƼã‚ºBleichenbacheræ”»æ’fæf…å ±æ¼ãã^ã„ã®è„†å¼±æ€§**

ãƒ¬ã‚¬ã‚·ãƼCisco ASA 5500ã‚·ãƒªãƼã‚ºï¼^ASA
5505ã€5510ã€5520ã€5540ã€ãŠã‚^ã³5550ï¼‰ãƒ‡ãƒã‚¤ã‚¹ã®TLSãƒ—ãƒƒãƒˆã‚³ãƒ«å®Ÿè£

ã“ã®è„†å¼±æ€§ã¯ãƒãƼã‚¸ãƒ§ãƒ³ã«RSAã‚’ä½¿ç”¨ã™ã‚‹æš—å·ã‚¹ãƒ¼ãƒˆã«å¯¾ã

ã“ã®è„†å¼±æ€§ã¯ãƒãƒªã‚¹ãƒˆã•ã‚Œã¦ã„ã„ASAãƒ¢ãƒ‡ãƒ«ã«Œ2048ãƒ“ãƒƒãƒˆRSAã‚ãƼã

ã�“ã�®è„†å¼±æ€§ã�«ã�¯CVE IDã�¨ã�—ã�¦CVE-2017-12373ã�Œå‰²ã,Šå½“ã�¦ã,‰ã,Œã�¦ã�„ã�¾ã�™ã€,

**SSLã�®å¯¯è¦–æ€§ã�«é–¢ã�™ã,‹Bleichenbacherã�®æ”»æ’ƒæ…å ±æ¼ã€ã€ã€

Cisco Product Security Incident Response
Teamï¼ˆPSIRTï¼‰ã€€æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªãƒ¼ã«è¨˜è¼‰ã•ã‚Œã¦ã„ã‚‹è„†å¼±æ€§

å‡ºå…¸

ã‚·ã‚¹ã‚³ã€Œã‚‰ã®è„†å¼±æ€§ã‚’å ±å‘Šã—ã¦ã„ãŸã ã„ãŸHanno
Böckæ°ã€Ruhr-Universität Bochum/Hackmanit GmbHã®Juraj
Somorovskyæ°ã€Tripwire VERTã®Craig
Youngæ°ã€ã‚Šã‚ˆã³testssl.sh/Drã®Dirk
Wetteræ°ã«æ„Ÿè¬ã„ãŸã—ã¾ã™ã€‚

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171212-bleichenbacher

æ”¹è¨‚å±¥æ´

ãƒãƒ¼ã‚¸ãƒ§ãƒ³	èª¬æ˜Ž
1.6	è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ã®æƒ…å ±ã‚’æ›´æ–°ã€CVE-2017-15533ã‚’è¿½åŠ ã€CVE-2017-17428ã®èª¬æ˜Žã‚’ä¿®æ£ã€ãƒ¦ãƒ¼ã‚¶ãƒ³ãƒˆã®ãƒ¦ãƒ¼ã‚¶ãƒ†ãƒ¼ãƒ–ãƒ«ã€ç„¡åŠ¹åŒ–
1.5	Cisco WebExè£½å“ã®æƒ…å ±ã¿ã«ãƒªãƒªãƒ¼ã‚¹ã•ã‚Œã€æƒ…å ±ã‚’æ›´æ–°ã€
1.4	Cisco ASAãƒ‡ãƒã‚¤ã‚¹ã®æƒ…å ±ã¿ã«ãƒªãƒªãƒ¼ã‚¹ã•ã‚Œã€å¯¾æ€§ã«é–¢
1.3	è„†å¼±æ€§ã®ã‚ã‚¨è„†å¼±æ€§ã®ãªã„è£½å“ã€CVE-2017-12373ã®èª¬æ˜Žã‚’ä¿®æ£ã€
1.2	è„†å¼±æ€§ã®ãªã„è£½å“ã«é–¢æ™‚ã€
1.1	è„†å¼±æ€§ã®ã‚¨è„†å¼±æ€§ã®ãªã„è£½å“ã€CVE-2017-12373ã‚’è¿½åŠ ã€
1.0	å^åžå…¬é–‹ãƒªãƒªãƒ¼ã‚¹

å^©ç”¨è¦ç´„

æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªãƒ¼ç„¡ä¿è¨¼ã®ã‚‚ã®ã¨ã—ã¦æ••ä¾›ã—ã¦ã„ã¾ã™ã€‚ã
æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªãƒ¼ã®æƒ…å ±ã®ä½¿ç”¨ã«é–¢ã™ã‚‹è²¬ä»»ã¯ã€ã
ã¾ãŸã€ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ãƒ¼ã®å†…å®¹ã‚’äº^å‘Šã•ã—ã«å¤‰æ›´ã—ã

æœ¬ã‚¢ãƒ‰ãƒ¬ã‚¹ã®è¨˜è¿°å†…容ã®¹ã«é–¢ã—ã¦æƒ…å ±é…ä¿¡ã® URL
ã‚’çœ•ç•¥ã—ã€€å˜ç‹¬ã®è»¢è¼‰ã„ã„„è¨³ã‚’æ–½ã—ã—ã¦ã„ã‚Ÿå´å˜ã€€å½“ç¤¾ã€Œç¡®
ã“ã®ãƒ‰ãƒ¡ã‚¤ãƒ³ãƒˆã®æƒ…å ±ã¯ã€·ã‚¹ã‚³è£½å“ã®ã¨ã¯ã‚‰ãƒ¦ãƒ¼ã‚¶ãƒ¼ã‚¬ã¯è±¡

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。