Cisco é�©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�Šã,ˆã�³ Firepower Threat Defense ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�® RSA ç§˜å¯†ã,ãƒ¼ãƒªãƒ¼ã,¯ã�®è„†å¼±æ€§

High

ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªãƒ¼ID : cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz

å^�å...¬é–‹æ—¥ : 2022-08-10 16:00

ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³ 1.0 : Final

CVSSã,¹ã,³ã,¢ : 7.4

å›žé�¿ç– : No workarounds available

Cisco ãƒ�ã,° ID : CSCwb88651 CSCwc28334

CVE-2022-20866

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

æ¦‚è¦

Cisco é�©å¿œåž‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƒ³ã,¹ï¼ˆASAï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�Šã,ˆã�³ Cisco Firepower Threat Defenseï¼ˆFTDï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,'å®Ÿè¡Œã�—ã�¦ã�„ã,‹ãƒ‡ãƒ�ã,¤ã,¹ã�§ã�® RSA ã,ãƒ¼ã�®å‡¦ç�†ã�®è„†å¼±æ€§ã�«ã,^ã,Šã€�èª�è¨¼ã�•ã,Œã�¦ã�„ã�ªã�„ãƒªãƒ¢ãƒ¼ãƒˆã�® RSA ç§˜å¯†ã,ãƒ¼ã,'å�–å¾—ã�™ã,‹å¯èƒ½æ€§ã�Œã�,ã,Šã�¾ã�™ã€,

ã�“ã�®è„†å¼±æ€§ã�¯ã€�ãƒ�ãƒ¼ãƒ‰ã,¦ã,§ã,¢ãƒ™ãƒ¼ã,¹ã�®æš—å�·åŒ–ã,'å®Ÿè¡Œã�™ã,‹ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã,©ãƒ¼ãƒ ã�®ãƒ¡ãƒ¢ãƒªã�« RSA ã,ãƒ¼ã�Œä¿�å˜ã�•ã,Œã�¦ã�„ã,‹ã�¨ã��ã�®è«–ç�†ã,¨ãƒ©ãƒ¼ã�«èµ·å› ã�—ã�¾ã�™ã€,æ Lenstra ã,µã,¤ãƒ‰ãƒ�ãƒ£ãƒ«æ”»æ'ƒã,'ä»•æŽ›ã�'ã�¦ã€�ã�“ã�®è„†å¼±æ€§ã,'æ,ªç"¨ã�™ã,‹å¯¯èƒ½æ€§ã,ã,Šã€,æ”»æ'ƒè€…ã,ç§˜å¯†ã,ãƒ¼ã,'å�–å¾—ã�§ã��ã,‹ã,^ã�†ã�«ã�ªã,Šã�¾ã�™ã€,

å½±éŸ¿ã,'å�—ã�'ã,‹ãƒ‡ãƒ�ã,¤ã,¹ã�§ã�¯ã€�æ¬¡ã�®çŠ¶æ…‹ã�Œè¦³å¯Ÿã�•ã,Œã,‹ã�“ã�¨ã�Œ

- ã�“ã�®è„†å¼±æ€§ã�¯ã€�Cisco ASAã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�¾ã�Ÿã�¯Cisco FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®è„†å¼±æ€§ã�®ã�,ã,‹ãƒªãƒªãƒ¼ã,¹ã,'å®Ÿè¡Œã�—ã�¦ã�„ã,‹ãƒ‡ãƒ

%ã«é©ç”¨ã•ã,Œã¾ã™ã€,RSAã,ãƒ¼ã«é©ç”¨ã•ã,Œã,‹æ•°å¦šã„è¨^ç®—ã«ã,

- **RSA ã,ãƒ¼ã€Œæœ‰åŠ¹ã§ã,ã£ã¦ã¦ã,,ã€RSA ç§˜å¯†ã,ãƒ¼ã®æ½œåœ¨çš„ãªãƒªã‚¯ã,¯ã«å¯¾ã™ã,‹è„†å¼±æ€§ã,'ç¤ºã™ã€ç‰**
  RSA ç§˜å¯†ã,ãƒ¼ã,'å®–å¾—ã™ã,‹ã¨ã€ã€ã••ã,ãƒ¼ã,'ä½¿ç”¨ã—ã¦ã€Cisco ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã¾ã€Ÿã¯ Cisco FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,'å®Ÿè¡Œã—ã¦ã„ã,‹ãƒ‡ãƒã,¤ã,¹ã«ã•ãŠã™ã¾ã™ã‹ã€ãƒ RSA ã,ãƒ¼ã®æ¤œå‡ºã®è©³ç´°ã«ã¤ã„ã¦ã¯ã€ä¾‹å®³ã€…ã€»ã,¯ã,·ãƒ
- RSA ã,ãƒ¼ã®å½¢å¼ã«æ£ã—ã••ã•ãªã€ç„¡åŠ¹ã§ã,ã,‹å¯èƒ½æ€§ã,Šã RSA ã,ãƒ¼ã¯æ©Ÿèƒ½ã›ã€ä¸æ£ãªå½¢å¼ã® RSA ã,ãƒ¼ã,'ä½¿ç”¨ã™ã,‹ Cisco ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã¾ã€Ÿã¯ Cisco FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,'å®Ÿè¡Œã—ã¦ã„ã,‹ãƒ‡ãƒã,¤ã,¹ã« TLS ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆæŽ¥ç¶šã,'è¡Œã†ã¨ã€TLS ç½²å••ã,¨ãƒ©ãƒ¼ã,'å¼•ã••èµ·ã“ã—ã¾ã™ã€,ã“ã,Œã¯ã€è„†å¼±ã•ã,½ãƒ•ãƒˆ RSA ç½²å••ã,'使ç”¨ã—ã€æ¤œè¼¼ã«å¤±æ•—ã™ã,‹ã“ã¨ã,'æ„•å³ã—ã¾ã™ RSA ç§˜å¯†ã,'å®–å¾—ã™ã,‹ã¨ã€ã€ã••ã,ãƒ¼ã,'ä½¿ç”¨ã—ã¦ã€Cisco ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã¾ã€Ÿã¯ Cisco FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,'å®Ÿè¡Œã—ã¦ã„ã,‹ãƒ‡ãƒã,¤ã,¹ã«ã•ãŠã™ã¾ã™ã‹ã€ãƒ

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¯ã€æ¬¡ã®ãƒªãƒ³ã,¯ã,^ã,Šç¢ºèªã§ã§ã¾ã™ã€,
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz

è©²å½“è£½å“

è„†å¼±æ€§ã®ã,ã,‹è£½å“

ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã,'å—ã‘ã,‹ã®ã¯ã€ãƒ‡ãƒã,¤ã,¹ã®ç¾åœ¨ã®è¨å®šã«ã,Cisco ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã¾ã€Ÿã¯ Cisco FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã,'å®Ÿè¡Œã—ã¦ã„ã,‹å ´å€ˆã®ã§ã™ã€,

- ASA 5506-X with FirePOWER ã,µãƒ¼ãƒ“ã,¹
- ASA 5506H-X with FirePOWER ã,µãƒ¼ãƒ“ã,¹
- ASA 5506W-X with FirePOWER ã,µãƒ¼ãƒ“ã,¹
- ASA 5508-X with FirePOWER ã,µãƒ¼ãƒ“ã,¹

- ASA 5516-X with FirePOWER ã‚µãƒ¼ãƒ“ã‚¹
- Firepower 1000 ã‚·ãƒªãƒ¼ã‚ºæ¬¡ä¸–代ファイアウォール
- FirePOWER 2100 ã‚·ãƒªãƒ¼ã‚º ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ ã‚¢ãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹
- FirePOWER 4100 ã‚·ãƒªãƒ¼ã‚º ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ ã‚¢ãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹
- FirePOWER 9300 ã‚·ãƒªãƒ¼ã‚º ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ ã‚¢ãƒ—ãƒ©ã‚¤ã‚¢ãƒ³ã‚¹
- Cisco Secure Firewall 3100

Additional Information:

- ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’å—ã‘ã‚‹ã®ã¯ã€Cisco ASAã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹9.16.1ä»¥é™ã®ã‚ˆã†Cisco FTDã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹7.0.0ä»¥é™ã® ã‘ã§ã§™ã€ã‚‚ã‚‰ä»¥å‰ã®ã®ã Cisco ASA ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ 9.15 ä»¥å‰ã¾ãŸã¯ Cisco FTD ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒªãƒªãƒ¼ã‚¹ 6.7 ä»¥å‰ã‚’実行ã—ã¦ã„ã‚‹å ´åˆã€ãƒ‡ãƒã‚¤ã‚¹ãŒã€å˜åœ¨ã™ã‚‹ RSA ã‚ãƒ¼ãƒšã‚¢ã®é•·ã•ã«ã¦ç”Ÿæˆ•ã•ã‚Œã¦ã
- ã“ã®è„†å¼±æ€§ã¯RSA ã‚ãƒ¼ãƒšã‚¢ã®æ¥•å††æ›²ç·šãƒã‚¸ãƒ«ç½²åã‚¢ãƒ«ã‚´ãƒªã‚
- ã“ã®è„†å¼±æ€§ã¯è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã‚’使用ã—ã¦ RSA ã‚ãƒ¼ãƒšã‚¢ã«å½±éŸ¿ã—ã¾ã™ã€‚ã¤ã¾ã‚Šã€è¨¼æ˜Žæ›¸ã¯ã€ç½²åã«ãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã‚’使用ã—ã¦ RSA ã‚ãƒ¼ãƒšã‚¢ã«å½±éŸ¿ã‚’与ãˆã‚‹å ´åˆã«è„†å¼±ã§ã™ã€‚ç§˜å¯†ãƒãƒƒã‚·ãƒ¥ã¯ã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã›ã‚“ã€‚

    - è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ç”Ÿæˆ•ã•ã‚Œ RSA ã‚ãƒ¼ã‚’ã‚µãƒãƒ¼ãƒˆã—ã¾ã™
    - ä»¥å‰ã®è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA ã‚ãƒ¼ãƒšã‚¢ã‚’使用ã—ã¦ã„ã‚‹ãƒ‡ãƒã‚¤ã‚¹ã§ã¯ã€ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰å¾Œã
    - è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA ã‚ãƒ¼ã‚’ã‚µãƒãƒ¼ãƒˆã—ã¾ã™ã€‚ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã§ã¯ã€è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ç”Ÿæˆ•ã•ã‚Œã¦ã„ã‚‹ãƒ‡ãƒã‚¤ã‚¹è¨¼æ˜Žæ›¸ã®ã¿ãŒå½±éŸ¿ã‚’受ã‘ã¾ã™ã€‚

ã—ãŸãŒã£ã¦ã€è„†å¼±æ€§ã®ã‚ã‚‹ãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA ã‚ãƒ¼ã‚’æœ€åˆ«ã«ç”Ÿæˆ•ã•ã‚Œã‚‹ã‚¢ã‚¤ãƒ‡ãƒ³ãƒ†ã‚£ãƒ†ã‚£è¨¼æ˜Žæ›¸ã®ã¿ãŒã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã™ã€‚è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA ã‚ãƒ¼ãƒšã‚¢ã§ç½²åã•ã‚Œã¦ã„ã‚‹è¨¼æ˜Žæ›¸ã®ã¿ãŒã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã™ã€‚ç§˜å¯†ãƒãƒƒã‚·ãƒ¥ã¯ã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã›ã‚“ã€‚è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ç”Ÿæˆ•ã•ã‚Œã¦ã„ã‚‹ãƒ‡ãƒã‚¤ã‚¹è¨¼æ˜Žæ›¸ã¯ã€ç½²åã«ãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã‚’使用ã—ã¦ RSA ã‚ãƒ¼ãƒšã‚¢ã«å½±éŸ¿ã‚’与ãˆã‚‹å ´åˆã«è„†å¼±ã§ã™ã€‚ç§˜å¯†ãƒãƒƒã‚·ãƒ¥ã¯ã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã›ã‚“ã€‚è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA ã‚ãƒ¼ãƒšã‚¢ã§ç½²åã•ã‚Œã¦ã„ã‚‹è¨¼æ˜Žæ›¸ã®ã¿ãŒã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã™ã€‚ç§˜å¯†ãƒãƒƒã‚·ãƒ¥ã¯ã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã›ã‚“ã€‚

    - è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ç”Ÿæˆ•ã•ã‚Œ RSA ã‚ãƒ¼ã‚’ã‚µãƒãƒ¼ãƒˆã—ã¾ã™
    - ä»¥å‰ã®è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA ã‚ãƒ¼ãƒšã‚¢ã‚’使用ã—ã¦ã„ã‚‹ãƒ‡ãƒã‚¤ã‚¹ã§ã¯ã€ã‚¢ãƒƒãƒ—ã‚°ãƒ¬ãƒ¼ãƒ‰å¾Œã
    - è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA

ã—ãŸãŒã£ã¦ã€è„†å¼±æ€§ã®ã‚ã‚‹ãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA ã‚ãƒ¼ã‚’最åˆ«ã«ç”Ÿæˆ•ã•ã‚Œã‚‹ã‚¢ã‚¤ãƒ‡ãƒ³ãƒ†ã‚£ãƒ†ã‚£è¨¼æ˜Žæ›¸ã®ã¿ãŒã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã™ã€‚è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ RSA ã‚ãƒ¼ãƒšã‚¢ã§ç½²åã•ã‚Œã¦ã„ã‚‹è¨¼æ˜Žæ›¸ã®ã¿ãŒã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã™ã€‚ç§˜å¯†ãƒãƒƒã‚·ãƒ¥ã¯ã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾ã›ã‚“ã€‚è„†å¼±ãªãƒãƒƒã‚·ãƒ¥ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã§ç”Ÿæˆ•ã•ã‚Œã¦ã„ã‚‹ãƒ‡ãƒã‚¤ã‚¹è¨¼æ˜Žæ›¸ã®ã¿ãŒã€ã“ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’受ã‘ã¾

è„†å¼±æ€§ã®å˜åœ¨ã™ã‚‹è¨å®š

ã,·ã,¹ã,³ã®ã,ªãƒ•ãƒœãƒƒã,¯ã,¹æ¤œå‡ºã,¹ã,¯ãƒªãƒ—ãƒˆã€�ã�¾ã�Ÿã�¯æœ¬ã,¢ãƒ‰ãƒ�ã,¤ã,
RSA ã,ãƒ¼ã�«ãƒ•ãƒ©ã,°ã�Œè¨å®šã�•ã,Œã�Ÿå ´å�ˆã€�RSA
ã,ãƒ¼ã,'ç½®æ››ã�—ã€�ã�"ã�® RSA
ã,ãƒ¼ãƒšã,¢ã,'ä½¿ç"¨ã�™ã,‹è¨¼æ˜Žæ›¸ã,'å¤±åŠ¹ã�•ã›ã€�äº¤æ››ã�™ã,‹ã�"ã�¨ã,'æŽ¨å¥¨ã
ASAã�Šã,^ã�³FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®æ©Ÿèƒ½ã�¯ã€�è¨å®šæ¸ˆã�¿ã�®RSAã,ãƒ¼ã�¨ã

ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

æ¬¡ã�®è¡¨ã�®å·¦å´ã�®åˆ—ã�«ç¤ºã�™ Cisco ASA
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã�®æ©Ÿèƒ½ã�¯ã€�ä¸€æ£ã�ªå½¢å¼�ã�¾ã�Ÿã�¯å½±éŸ¿ã,'å�—ã�'ã
RSA
ã,ãƒ¼ã�Œã��ã�®æ©Ÿèƒ½ã�®è¨å®šã�«é–¢é€£ä»˜ã'ã,‰ã,Œã�¦ã�„ã,‹å ´å�ˆã�«ã€�è„
running-config CLI
**ã,³ãƒžãƒ³ãƒ‰ã�§å^¤æ–å�¯èƒ½ã�ªã€�ã"ã®æ©Ÿèƒ½ã®åŸºæœ¬è¨å®šã,'ç¤ºã—ã¾¾

Cisco ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®æ©Ÿèƒ½	è„†å¼±æ€§ã®
Adaptive Security Device Managerï¼^ASDMï¼‰[1]	`http server enable <por` `http <remote_ip_address`
AnyConnect SSL VPN	`webvpn` ` enable <interface_name`
Cisco Security Managerï¼^CSMï¼‰[1]	`http server enable <por` `http <remote_ip_address`
ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆãƒ¬ã,¹ SSL VPNï¼^WebVPNï¼‰[2]	`webvpn` ` enable <interface_name`

è¨¼æ˜Žæ›¸ãƒ™ãƒ¼ã,¹ã�®èª�è¨¼ã,'ä½¿ç"¨ã�—ã�Ÿã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã‚§ãƒ¼ã,ãƒ¼ ã,¨ã,¯ã,¹ãƒ•ã,§ãƒ³ã,¸ ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³ 1ï¼^IKEv1ï¼‰VPNï¼^ãƒªãƒ¢ãƒ¼ãƒˆã,¢ã,¯ã,»ã,¹ã�Šã,^ã�³ LAN-to-LANï¼‰	`crypto ikev1 enable <in`
	`crypto ikev1 policy <pr`
	` authentication rsa-sig`
	`tunnel-group <tunnel_gr`

Cisco ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®®æ©Ÿèƒ½	è„†å¼±æ€§ã®®
	trust-point <trustpoi
è¨¼æ˜Žæ›¸ãƒ™ãƒ¼ã,¹ã®®èª è¨¼ã,'ä½¿ç"¨ã—ã—Ÿã,¤ãƒ³ã,¿ãƒ¼ãƒ•ã‚§ãƒ¼ã,ãƒ¼ ã,¨ã,¯ã,¹ãƒ•ã,§ãƒ³ã,¸ ãƒ•ãƒ¼ã,¸ãƒ§ãƒ³ 2ï¼ˆIKEv2ï¼‰VPNï¼ˆãƒªãƒ¢ãƒ¼ãƒˆã,¢ã,¯ã,»ã,¹ã•Šã,ˆã•³ LAN-to-LANï¼‰	crypto ikev2 enable <in tunnel-group <tunnel_gr ikev2 remote-authentic ikev2 local-authentica
Proxy Bypass	webvpn proxy-bypass
TLS ãƒ—ãƒã,·	tls-proxy <name>
REST API[1]	rest-api image disk0:/ rest-api agent
SSH ã,¢ã,¯ã,»ã,¹[3]	ssh <remote_ip_address>

1. ASDMã€•CSMã€•ã•Šã,ˆã•³ REST API ã,µãƼãƒ"ã,¹ã•¯ã€• **http**
ã,³ãƒžãƒ³ãƒ‰ã•§è¨å®šã••ã,Œã•Ÿç¯„å›²ã•® IP
ã,¢ãƒ‰ãƬ¬ã,¹ã•‹ã,‰ã•®ã•¿ã,¢ã,¯ã,»ã,¹ã•§ã••ã•¾ã•™ã€,
2. ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆãƬ¬ã,¹ SSL VPN ã•¯ã€•Cisco ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƼ¼ã,¹ 9.17(1)
ä»¥é™•ã•§ã•¯ã,µãƒ•ãƼãƒˆã••ã,Œã•ªã••ã•ªã,Šã•¾ã•—ã•Ÿã€,
3. SSH ã,µãƼãƒ"ã,¹ã•¯ã€• **ssh** ã,³ãƒžãƒ³ãƒ‰ã•§è¨å®šã••ã,Œã•Ÿç¯„å›²ã•® IP
ã,¢ãƒ‰ãƬ¬ã,¹ã•‹ã,‰ã•®ã•¿ã,¢ã,¯ã,»ã,¹ã•§ã••ã•¾ã•™ã€,

FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

æ¬¡ã•®è¡¨ã•®å·¦å•´ã•®åˆ—ã•«ç¤ºã•™ Cisco FTD
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®æ©Ÿèƒ½ã•¯ã€•ä¸•æ£ã•ªå½¢å¼•ã•¾ã•Ÿã•¯å½±éŸ¿ã,'å•—ã•'ã
RSA
ã,ãƼ¼ã•Œã••ã•®æ©Ÿèƒ½ã•®è¨å®šã•«é–¢é€£ä»˜ã•'ã,‰ã,Œã•¦ã•„ã,‹å ´å•ˆã•«ã€•è„

running-config CLI

ã,³ãƒžãƒ³ãƒ‰ã§å^¤æ–å¯¯èƒ½ã•ã€ã"ã®æ©Ÿèƒ½ã®åŸºæœ¬è¨å®šã,'ç¤ºã—ã¾ã

Cisco FTD æ©Ÿèƒ½	è„†å¼±æ€§ã®å¯¯èƒ½æ€§ã‚Œã,ã
AnyConnect SSL VPN[1ã€‚2]	webvpn enable <interface_name>
ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆãƒ¬ã,¹ SSL VPNï¼^WebVPNï¼‰[2]	webvpn enable <interface_name>
è¨¼æ˜Žæ›¸ãƒ™ãƒ¼ã,¹ã•®èª•è¨¼ã,'ä½¿ç"¨ã—ãŸ IKEv1 VPNï¼^ãƒªãƒ¢ãƒ¼ãƒˆã,¢ã,¯ã,»ã,¹ã•Šã,^ã•³ LAN-to-LANï¼‰[1ã€‚2]	crypto ikev1 enable <interface_name> crypto ikev1 policy <priority> authentication rsa-sig tunnel-group <tunnel_group_name> ipsec-attribu trust-point <trustpoint_name>
è¨¼æ˜Žæ›¸ãƒ™ãƒ¼ã,¹ã•®èª•è¨¼ã,'ä½¿ç"¨ã—ãŸ IKEv2 VPNï¼^ãƒªãƒ¢ãƒ¼ãƒˆã,¢ã,¯ã,»ã,¹ã•Šã,^ã•³ LAN-to-LANï¼‰[1ã€‚2]	crypto ikev2 enable <interface_name> tunnel-group <tunnel_group_name> ipsec-attribu ikev2 remote-authentication certificate ikev2 local-authentication certificate <trust

1. ãƒªãƒ¢ãƒ¼ãƒˆã,¯ã,»ã,¹ VPN æ©Ÿèƒ½ã•¯ã€•Cisco Firepower Management Centerï¼^FMCï¼‰ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•§ [ãƒ‡ãƒ•ã,¤ã,¹ï¼^Devicesï¼‰] > [VPN] > [ãƒªãƒ¢ãƒ¼ãƒˆã,¢ã,¯ã,»ã,¹ï¼^Remote Accessï¼‰] ã•®é †ã•«é•¸æŠžã•™ã,‹ã•‹ã€•ã•¾ã•Ÿã•¯ Cisco Firepower Device Managerï¼^FDMï¼‰ã•§ [ãƒ‡ãƒ•ã,¤ã,¹ï¼^Devicesï¼‰] > [ãƒªãƒ¢ãƒ¼ãƒˆã,¢ã,¯ã,»ã,¹VPNï¼^Remote Access VPNï¼‰] ã•®é †ã•«é•¸æŠžã•™ã,‹ã•¨æœ‰åŠ¹ã•«ã•ªã,Šã•¾ã•™ã€,

2.ã,¯ãƒ©ã,¤ã,¢ãƒ³ãƒˆãƒ¬ã,¹SSL VPNæ©Ÿèƒ½ã•¯ã€•Cisco FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹7.1.0ã•§ã•¯ã,µãƒ•ãƒ¼ãƒˆã••ã,Œã•¦ã•„ã•¾ã•›ã,"ã€,ã•Ÿ FTDã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã•§ã•¯ã€•FlexConfigã,'ä½¿ç"¨ã—ã•¦æœ‰åŠ¹ã•«ã•§ã•

RSA

ã,ãƒ¼ã•Œä¸•æ£ã•ªå½¢å¼•ã•§ã•,ã,‹ã•‹ã€•å½±éŸ¿ã,'å•—ã•'ã,„ã•™ã•

RSA

ã,ãƒ¼ã•Œä¸•æ£ã•ªå½¢å¼•ã•§ã•,ã,‹ã•‹å½±éŸ¿ã,'å•—ã•'ã,„ã•™ã•„ã•‹ã•©ã•†ã•‹ã,'å
ç§˜å¯†ã,ãƒ¼ãƒªãƒ¼ã,¯ã•®å•¯èƒ½æ€§ã•Œã•,ã,‹ã€•ä¸•æ£ã•ªå½¢å¼•ã•¾ã•Ÿã•¯å½±éŸ¿ã
RSA
ã,ãƒ¼ã,'æ¤œå‡ºã•—ã•¾ã•™ã€,é¡§å®¢ã•¯ã€•æ©Ÿå¯†ã,ãƒ¼æƒ…å ±ã,'é¡§å®¢ã•®ç°å¢ƒã•‹ã,
ASA ã•¾ã•Ÿã•¯ FTD
ãƒ‡ãƒ•ã,¤ã,¹ã•§ã•¯ã•ªã••ï¼‰ã•§ã•“ã•®ã,¹ã,¯ãƒªãƒ—ãƒˆã,'å®Ÿè¡Œã•§ã••ã•¾ã•™ã€

ãƒ‡ãƒ•ã,¤ã,¹ã•Œ Cisco ASA ã•¾ã•Ÿã•¯ FTD
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•®è„†å¼±æ€§ã•®ã•,ã,‹ãƒªãƒªãƒ¼ã,¹ã,'å®Ÿè¡Œã•—ã•¦ã•Šã,Šã€•ä¿®æ£

ã,¹ã,¯ãƒªãƒ—ãƒˆã,'使ç”¨ã•™ã,‹ã•«ã•¯ã€•æ¬¡ã•®æ‰‹é †ã,'å®Ÿè¡Œã•—ã•¾ã•™ã€,

1. å½±éŸ¿ã,'å•—ã•'ã,‹å•¯èƒ½æ€§ã•®ã•,ã,‹ãƒ‡ãƒ•ã,¤ã,¹ã•‹ã,‰ã€•ãƒ†ã,¹ãƒˆã•Œå¿…è¦
   RSA ã,ãƒ¼ã,'ã,¨ã,¯ã,¹ãƒ•ãƒ¼ãƒˆã•—ã•¾ã•™ã€,
2. ã,¹ã,¯ãƒªãƒ—ãƒˆã,'å®Ÿè¡Œã•—ã•¦ã€•ã•šã,Œã•‹ã•® RSA
   ã,ãƒ¼ã•Œä¸•æ£ã•ªå½¢å¼•ã•§ã•,ã,‹ã•‹ã€•RSA
   ç§˜å¯†ã,ãƒ¼ãƒªãƒ¼ã,¯ã•®å½±éŸ¿ã,'å•—ã•'ã,„ã•™ã•„ã•‹ã•©ã•†ã•‹ã,'ç‰¹å®šã•—ã

ã,¹ã,¯ãƒªãƒ—ãƒˆã•Šã,^ã•³é–¢é€£ã•™ã,‹ãƒ‰ã,ãƒ¥ãƒ¡ãƒ³ãƒˆã•«ã•¤ã•„ã•¦ã•¯ã€•https://github.c
2022-20866 ã,'å•,ç…§ã•—ã•¦ã••ã• ã••ã•„ã€,

æ³¨:RSAã,ãƒ¼ã•Œç•¾åœ¨è¨¬å®šã••ã,Œã•¦ã•„ã•ªã•„ã•Œã€•è„†å¼±æ€§ã•®ã•,ã,‹ã,½ãƒ
RSA ã,ãƒ¼ã,'å‰Šé™¤ã•—ã€•ã•"ã•® RSA
ã,ãƒ¼ãƒšã,¢ã,'ä½¿ç"¨ã•™ã,‹è¨¼æ˜Žæ›¸ã,'ã•™ã•¹ã•¦ç„¡åŠ¹ã•«ã•™ã,‹ã•"ã•¨ã•Œæ˜¯å¥¨ã•

è„†å¼±æ€§ã,'å•«ã,"ã•§ã•„ã•ªã•„ã•"ã•¨ã•Œç¢ºèªã•§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,¹ã,³ã•¯ã€•ã•"ã•®è„†å¼±æ€§ã•Œ Cisco FMC
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã•«ã•¯å½±éŸ¿ã,'ä¸Žã•^ã•ªã•„ã•"ã•¨ã,'ç¢ºèªã••ã•—ã•¾ã•—ã•Ÿã€

è©³ç´°

Lenstra æ”»æ’ƒ

1996 å¹´ã€•Arjen Lenstra
æ°•ã•«ã,^ã,Šã€•ä¸›ã•®å‰°ä½™å®šç•†æœ€é•©åŒ–ï¼^RSA-
CRTï¼‰ã•«å¯¾ã•™ã,‹æ”»æ’ƒã•Œèª¬æ˜Žã••ã,Œã•¾ã•—ã•Ÿã€,RSA-CRT
æœ€é•©åŒ–ã•®ä½¿ç"¨æ™‚ã•«ã€•æš—å•·ç½²å••ã•®è¨^ç®—ä¸ã•«éšœå®³ã•Œç™ºç”Ÿã•
CRT ã,ãƒ¼ãƒªãƒ¼ã,¯ã•¨ã,µå'¼ã•°ã,Œã•¾ã•™ã€,Lenstra
æ”»æ’ƒã•¯ã€•ã,^ã••çŸ¥ã,‰ã,Œã•Ÿã,µã,¤ãƒ‰ãƒ•ãƒ£ãƒ•ãƒ«æ”»æ’ƒã•§ã•™ã€,RSA

ã,¢ãƒ«ã,´ãƒªã,ºãƒ ã,'ç›´æŽ¥æ"»æ'ƒã€™ã,‹ã€"ã€¨ã€¯ã€,ã,Šã€¾ã€›ã,"ã€Œã€€å®Ÿè£…ã€®æ¬ é

æ"»æ'ƒã€®è©³ç´°ã€«ã€¤ã€„ã€¦ã€¯ã€€ã€Œ[Memo on RSA signature generation in the presence of faults](#)ã€€ã,'å€,ç…§ã€—ã€¦ã€€ã€•ã€„ã€,

æœ¬ã,¢ãƒ‰ãƒ€ã,¤ã,¶ãƒªã€§è¤æ˜Žã€•ã,Œã€¦ã€„ã,‹è„†å¼±æ€§ã€«ã,^ã,Šã€€RSA ã,ãƒ¼ã€§ Lenstra ã,µã,¤ãƒ‰ãƒ€ãƒ£ãƒ€ãƒ«æ"»æ'ƒã€Œæ^€åŠŸã€—ã€€æ"»æ'ƒè€…ã€Œ RSA ç§˜å¯†ã,ãƒ¼ã,'å€–å¾—ã€§ã€€ã,‹å€¯èƒ½æ€§ã€Œã€,ã,Šã€¾ã€™ã€,

ã,»ã,ãƒ¥ãƒªãƒ†ã,£ä¾µå®³ã€®ç—•è·¡

ã€"ã,Œã,‰ã€®ä¾µå®³ã€®å…†å€™ã€¯ã€€ä¿®æ£æ¸ˆã€¿ã€® Cisco ASA ã€¾ã€Ÿã€¯ FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã€§ã€®ã€¿ç¢ºèª€ã€§ã€€ã€¾ã€™ã€,ä»¥å‰€ã€®ã,½ãƒ•ãƒˆã,

å½±éŸ¿ã,'å€—ã€'ã,‹ãƒ‡ãƒ€ã,¤ã,¹ã€Œä¿®æ£æ¸ˆã€¿ã€®ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã€«ã,¢ãƒƒã ç§˜å¯†ã,ãƒ¼ãƒªãƒ¼ã,¯ã€®å€¯èƒ½æ€§ã€®ã€,ã,‹ RSA ã,ãƒ¼ã€Œãƒ‡ãƒ€ã,¤ã,¹ã€«å˜åœ¨ã€™ã,‹ã€"ã€¨ã,'ç®¡ç€†è€…ã€«è¦å'Šã€—ã€¾ã€™ã€,

ä¿®æ£æ¸ˆã€¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã€¸ã€®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰æ¨ RSA ã,ãƒ¼ã,'æ¤œå‡ºã€™ã,‹æ–¹æ³•

é‡€å¤§ãƒ¬ãƒ™ãƒ«ã€® Syslog ãƒ¡ãƒƒã,»ãƒ¼ã,¸

å½±éŸ¿ã,'å€—ã€'ã,‹ãƒ‡ãƒ€ã,¤ã,¹ã€Œä¿®æ£æ¸ˆã€¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã€«ã,¢ãƒƒãƒ—ã, RSA ã,ãƒ¼ã€Œæ¤œå‡ºã€•ã,Œã€Ÿå ´å^ã€€2 ã€¤ã€®æ–°ã€—ã€„ syslog ãƒ¡ãƒƒã,»ãƒ¼ã,¸ã€«ã,^ã€£ã€¦ç®¡ç€†è€…ã€«è¦å'Šã€Œç™ºã€›ã,‰ã,Œã€¾ã€™ã€,ã€"ã,Œã,‰ã€ RSA ã,ãƒ¼ã€§ RSA ç§˜å¯†ã,ãƒ¼ã€Œæ¼€æ´©ã€—ã€Ÿå€¯èƒ½æ€§ã€Œã€,ã,‹ã€"ã€¨ã,'æ„€å'³ã€—ã€¾ã€™ã€,æ- syslog ãƒ¡ãƒƒã,»ãƒ¼ã,¸ã€¯é‡€å¤§ãƒ¬ãƒ™ãƒ«ã€§è¨˜éŒ²ã€•ã,Œã€€ç®¡ç€†è€…ã€Œ **show logging** CLI ã,³ãƒžãƒ³ãƒ‰ã,'使ç"¨ã€™ã,‹ã€"ã€¨ã€§ç¢ºèª€ã€§ã€€ã€¾ã€™ã€,**ASA** ã€¾ã€Ÿã€¯ **FTD** ã€®ãƒ—ãƒ¬ãƒ•ã,£ãƒƒã,¯ã,¹ã€¯ã€€syslog ã€Œè¡¨ç¤ºã€•ã,Œã€¦ã€„ã,‹ãƒ‡ãƒ€ã,¤ã,¹ã€®ã,¿ã,¤ãƒ—ã€«å›ºæœ‰ã€§ã€™ã€,æ-°ã€—ã€„ syslog ãƒ¡ãƒƒã,»ãƒ¼ã,¸ã€¯æ¬¡ã€®ã,^ã€†ã€«è¡¨ç¤ºã€•ã,Œã€¾ã€™ã€,

%ASA-1-717065:Keypair <name>ã€¯Cisco RSAç§˜å¯†ã,ãƒ¼æ¼€æ´©ã€®è„†å¼±æ€§(CVE-2022-20866)ã€«ã,^ã,Šç„¡åŠ¹ã€§ã€,ã,Šã€€ãƒ¡ãƒ¢ãƒªå†…ã€§ã,¯ãƒªã,¢ã€•ã,Œã€¾ã€™ã€,ã€"ã€®ã

%FTD-1-717065:Keypair <name>ã€¯ã€€Cisco RSAç§˜å¯†ã,ãƒ¼æ¼€æ´©ã€®è„†å¼±æ€§(CVE-2022-20866)ã€ŒåŽŸå› ã€§ç„¡åŠ¹ã€§ã€,ã,Šã€€ãƒ¡ãƒ¢ãƒªå†…ã€§ã,¯ãƒªã,¢ã€•ã,Œã€¾ã€™ã€,ã€"

Syslog ãƒ¡ãƒƒã‚»ãƼã‚¸ **ASA-1-717065** ã€Šã‚ˆã€‹ **FTD-1-717065**
ã€¯ã€€æœ¬ã‚»ã‚¯ã‚·ãƧãƪã‚£ã‚¢ãƒ‰ãƒ•ã‚¤ã‚¹ã€¶ãƪã€§è¬æ˜Žã——ã¦ã„ã‚‹ RSA
ç§˜å¯†ã‚ãƼãƪãƼã‚¯ã€¯ã«å¯¾ã——ã¦è„†å¼±æ€§ã®ã‚‹ã‚‹ä¸æ£å¥½å¼•ã®
RSA
ã‚ãƼã€Œæ¤œå‡ºã•ã‚Œã€Ÿã€“ã€¨ã‚’ç¤ºã——ã¦ã„ã¾ã™ã€‚ä¸æ£å¥½å¼•ã®
RSA
ã‚ãƼã€¯ç„¡åŠ¹ã«ã—ãªã„ã‚‹ã€Ÿã€€ä½¿ç”¨ã¨§ã€€ã¾ã›ã‚“ã€“ã€®
RSA
ã‚ãƼã€¯ã€“ã‚Œã¾ã§æ©Ÿèƒ½ã——ã¦ã„ãŠã‚‰ã€šç½®æ››ã™ã‚‹å¿…è¦ã€Œã€ã‚Š
RSA
ã‚ãƼãƚšã‚¢ã‚’ä½¿ç”¨ã™ã‚‹ã¨è¨¼æ˜Žæ›¸ã‚‚ã™ã¹ã¦å¤±åŠ¹ã•ã›ã€ä¤æ››ã™ã‚‹å¿…è¦ã€

%ASA-1-717066: Keypair <name>ã€¯æœ‰åŠ¹ã§ã™ã€Œã€Cisco RSAç§˜å¯†ã‚ãƼæ¼ã€ˆã€„ã€®è„†å¼±æ€§(CVE-2022-20866)ã€«ã‚ˆã‚Šã€€ä»¥å‰ã€®ãƒ•ãƼã‚¸ãƧãƳã€§ã€®å…¬é–‹ã€«å¯¾ã——ã¦è„†å¼±

%FTD-1-717066: Keypair <name>ã€¯æœ‰åŠ¹ã§ã™ã€Œã€Cisco RSAç§˜å¯†ã‚ãƼæ¼æ´©ã€®è„†å¼±æ€§(CVE-2022-20866)ã€«ã‚ˆã‚Šã€€ä»¥å‰ã€®ãƒ•ãƼã‚¸ãƧãƳã€®è„†å¼±æ€§ã€®å½±éŸ¿ã‚’å——ã‘ã€

Syslog ãƒ¡ãƒƒã‚»ãƼã‚¸ **ASA-1-717066** ã€Šã‚ˆã€‹ **FTD-1-717066** ã€¯ã€€RSA
ã‚ãƼã€¯ä¸æ£å¥½å¼•ã€§ã€¯ã€ªã€„ã€Œã€æœ¬ã‚»ã‚¯ã‚·ãƧãƪã‚£ã‚¢ãƒ‰ãƒ•ã‚¤ã‚¹ã€¶ãƪ
RSA
ç§˜å¯†ã‚ãƼãƪãƼã‚¯ã€¯ã€®å½±éŸ¿ã‚’å——ã‘ã„ã€™ã€„ã€“ã€¨ã‚’ç¤ºã——ã¦ã„ã€„ã€¾ã€™ã€€ã€
RSA ã‚ãƼã‚’ç½®æ››ã——ã€€ã€“ã€® RSA
ã‚ãƼãƚšã‚¢ã‚’ä½¿ç”¨ã——ã„ã‚‹ã€™ã€¹ã€¦ã€®è¨¼æ˜Žæ›¸ã‚’å¤±åŠ¹ã•ã›ã€ä¤æ››ã€

ã‚¨ãƩãƼ ã‚«ã‚¦ãƳã‚¿

å½±éŸ¿ã‚’å——ã‘ã‚‹ãƫãƒ‰ã‚¤ã‚¹ã‚¿ã€Œä¿®æ£æ¸ˆã¿ã‚½ãƒ•ãƈã‚¦ã‚§ã‚¢ãƪãƼã‚¹ã€«ã‚¢ãƫãƗã€
RSA
ã‚ãƼã€Œæ¤œå‡ºã•ã‚Œã€Ÿã‚‹ã€©ã€†ã‚‹ã€Œè¨¼ç¤ºã•ã‚Œã¾ã™ã€“ã€‚ã‚‰ã€®ã
counters | grep PKI CLI
ã‚³ãƞãƳãƉã‚’ä½¿ç”¨ã——ã€æ–°ã——ã„ã‚¨ãƼã‚«ã‚¦ãƳã‚¿ã€¯æ¬¡ã®ã‚ˆã†ã«è

<#root>

asaftd#

show counters | grep PKI

...

```
PKI          RSAKEY_INVAL_VULN                    1   Summary
PKI          RSAKEY_INVAL_SCRUB                   1   Summary
PKI          RSAKEY_INVAL_NOT_VULN                1   Summary
PKI          RSAKEY_VALID_SHORT                   1   Summary
PKI          RSAKEY_ANALYSIS_ERROR                1   Summary
PKI          RSAKEY_SCRUB_ERROR                   1   Summary
```

æ–°ã•—ã•„ã,¨ãƒ©ãƼã,«ã,¦ãƳã,¿ã•®ã••ã,Œã•žã,Œã•®æ„•å‘³ã•¯æ¬¡ã•®ã•¨ã•Šã,Šã•§ã

- **RSAKEY_INVAL_VULNï¼šç„¡åŠ¹ã•ªè„†å¼±**æ€§ã,ãƒ¼ã•Œæ¤œå‡ºã••ã,Œã•¾ã•—ã•Ÿ
- **RSAKEY_INVAL_SCRUBï¼šç„¡åŠ¹ã•ªè„†å¼±**æ€§ã,ãƒ¼ã•Œãƒ¡ãƒ¢ãƪã•§ã,¯ãƪã,¢ã••ã,Œã•¾
- **RSAKEY_INVAL_NOT_VULNï¼šç„¡åŠ¹ã•ª**ãƼã€•è„†å¼±ã•§ã•¯ã•,ã,Šã•¾ã•›ã,"
- **RSAKEY_VALID_SHORT**ï¼šå½±éŸ¿ã,'å•—ã•'ã,<ä»¥å‰•ã•®ãƒ•ãƼã,¸ãƒ§ãƳã•§ã•¯è„†å¼
- **RSAKEY_ANALYSIS_ERRORï¼šå^†æž•ä¸ã•«ã,¨ãƩãƼã•Œç™ºç"Ÿã•—ã•¾ã•—ã•Ÿ
- **RSAKEY_SCRUB_ERRORï¼šã,¹**ã,¯ãƒ©ãƼã•«ã,¨ãƩãƼã•Œç™ºç"Ÿã•—ã•¾ã•—

ã•"ã,Œã,‰ã•®ã,«ã,¦ãƳã,¿ã•¯ã€•å¯¾å¿œã•™ã,‹ syslog
ãƒ¡ãƒƪã,»ãƼã,¸ã•Œãƪã,°ã•«è¨˜éŒ²ã••ã,Œã•Ÿã••ã••ã•«å¢—å^†ã••ã,Œã•¾ã•™ã€,ã•¾ã•
RSA ã,ãƼã,'ç½®æ•›ã•—ã•¦ã€•RSA
ã,ãƼãƪã,¢ã,'ä½¿"¨ã•™ã,‹è¨¼æ˜Žæ›¸ã,'å¤±åŠ¹ã••ã•›ã€•ä°¤æ•›ã•™ã,‹ã•"ã••ã•Œå¿…è¦•ã

ãƒ‡ãƒ•ã,¤ã,¹ãƒ–ãƼãƈæ™,ã•®è¦å'Š

å½±éŸ¿ã,'å•—ã•'ã,‹ãƒ‡ãƒ•ã,¤ã,¹ã•Œä¿®æ£æ¸ˆã•¿ã,½ãƒ•ãƈã,¦ã,§ã,¢ãƪãƪãƼã,¹ã•«ã,¢ãƒƒãƗã,
RSA
ã,ãƼã•Œæ¤œå‡ºã••ã,Œã•Ÿå ´å•ˆã€•ãƒ–ãƼãƈã,·ãƼã,±ãƳã,¹ä¸ã•«æ¬¡ã•®ã,³ãƳã,½ãƼãƫãƪã
1 ã•¤ä»¥ä¸Šã•Œè¡¨ç¤ºã••ã,Œã,‹ã•"ã••ã•Œã•,ã,Šã•¾ã•™ã€,

CRITICAL:	RSA ã,ãƼ <name> ã•¯
	Cisco RSA ç§˜å¯†ã,ãƼãƪãƼã,¯ã•®è„†å¼±æ€§ï¼^CVE-2022-20866ï¼‰
	ã•Œå Ÿå› ã•§ç„¡åŠ¹ã•«ã•ªã,Šã€•ãƒ¡ãƢãƪã•‹ã,‰æ¶^åŽ»ã••ã,Œã•
CRITICAL:	RSA ã,ãƼ <name> ã•¯ä»¥ä¸‹ã•Œå Ÿå› ã•§
	ä»¥å‰•ã•®ãƒ•ãƼã,¸ãƒ§ãƳã•§ã,¨ã,¯ã,¹ãƒ•ãƼã,¸ãƒ£ã•«å¯¾ã•—ã•
	Cisco RSA ç§˜å¯†ã,ãƼãƪãƼã,¯ã•®è„†å¼±æ€§ï¼^CVE-2022-20866ï¼‰ã€,
	ã•"ã•®ã,ãƼã,'å‰Šé™¤ã•—ã•¦ã••ã• ã••ã•„ã€,

ã•"ã,Œã,‰ã•®ãƒ–ãƼãƈæ™,ã•®è¦å'Šã•"ã•¨ã•«ã€•å¯¾å¿œã•™ã,‹ syslog
ãƒ¡ãƒƪã,»ãƼã,¸ã•Œãƪã,°ã•«è¨˜éŒ²ã••ã,Œã¾ã•™ã€,ã•¾ã•Ÿã€•RSA
ã,ãƼã,'ç½®æ•›ã•—ã•¦ã€•RSA
ã,ãƼãƪã,¢ã,'ä½¿"¨ã•™ã,‹ã•™ã•¹ã•¦ã•®è¨¼æ˜Žæ›¸ã,'å¤±åŠ¹ã••ã•›ã•¦ä°¤æ•›ã•™ã,‹ã•"ã

ãƒ‡ãƒ•ãƒƒã‚°ãƒ¡ãƒ‹ãƒ¥ãƒ¼ã•®ã,³ãƒžãƒ³ãƒ‰

å½±éŸ¿ã,’å•—ã•‘ã,‹ Cisco ASA ã•¾ã•Ÿã•¯ FTD
ãƒ‡ãƒ•ã,¤ã,¹ã,’ä¿®æ£æ¸ˆã•¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã•«ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã•—ã•Ÿå
debug menu pki 60 ã,’ä½¿ç”¨ã•—ã•¦ã€•ãƒ‡ãƒ•ã,¤ã,¹ä¸Šã•®ã•™ã•¹ã•¦ã•® RSA
ã,ãƒ¼ã,’è§£æž•ã•—ã•¾ã•™ã€,ã,³ãƒžãƒ³ãƒ‰å‡ºåŠ›ã•«ã•¯ã€•å•„ RSA
ã,ãƒ¼ã•®çŠ¶æ…‹ã•Œè¡¨ç¤ºã••ã,Œã€•ã••ã,Œã,‰ã•®ã•„ã•šã,Œã•‹ã•Œä¾µå®³ã••ã,Œã
å^—ã•«ã•¯ã€•å•„ RSA
ã,ãƒ¼ã•®ç•¾åœ¨ã•®ã,¹ãƒ†ãƒ¼ã,¿ã,¹ã•Œè¡¨ç¤ºã••ã,Œã•¾ã•™ã€,ã•“ã•®å^—ã•®å€¤
INVALID ã•¯ã€•RSA
ç§˜å¯†ã,ãƒ¼ã•Œæ¼•æ´©ã•—ã•Ÿå•¯èƒ½æ€§ã•Œã•,ã,‹ã•“ã•¨ã,’ç¤ºã•—ã•¦ã•„ã•¾ã•™ã

```
asa# debug menu pki 60
Key Name                 : Validity  : Cisco RSA Malformed Key Vulnerability
                         :           : (CVE-2022-20866) exposure status
------------------------ : --------- : ------------------------------------
<Default-RSA-Key>        : Valid     : No exposure characteristics
test1                    : Valid     : ** Possible exposure in earlier software versions
test3                    : INVALID   : No exposure characteristics
test8                    : INVALID   : ** Key generated by affected version, cleared in memory
tets2                    : ERROR     : ** Error during analysis
test4                    : INVALID   : ** Has exposure characteristics
test5                    : unknown   : Key pair not analyzed
```

æ¤œå‡ºä¸è•ªä¸æ£ã•ªå½¢å¼•ã•® RSA ã,ãƒ¼

é•ŽåŽ»ã•«ä½¿ç”¨ã••ã,Œã•¦ã•••ã•®å¾Œå‰Šé™¤ã••ã,Œã•Ÿã€•ä¸•æ£ã•ªå½¢å¼•ã•¾ã•
RSA ã,ãƒ¼ã,’æ¤œå‡ºã•™ã,‹ã•“ã•¨ã•¯ã•§ã••ã•¾ã•›ã,“ã€,ä¸€éƒ¨ã•® RSA
ã,ãƒ¼ã•¯ã€•ä¸•æ£ã•ªå½¢å¼•ã•Œåžŷå› ã•§æ©Ÿèƒ½ã•—ã•¦ã•„ã•ªã•‹ã•£ã•Ÿã•Ÿã,•ã
RSA
ã,ãƒ¼ã•Œé•ŽåŽ»ã•«ãƒ‡ãƒ•ã,¤ã,¹ã•§ä½¿ç”¨ã••ã,Œã•¦ã•„ã•Ÿæ‡¸å¿µã•Œã•,ã,‹å ´å•^ã•¯ã€
RSA
ã,ãƒ¼ãƒšã,¢ã,’ä½¿ç”¨ã•—ã•¦ã•„ã,‹è¨¼æ˜Žæ›¸ã•Œã•™ã•¹ã•¦å¤±åŠ¹ã•—ã•¦ã•„ã,‹ã•“ã•¨ã

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,·ã,¹ã,³ã•¯ã•“ã•®ã,¢ãƒ‰ãƒ•ã,¤ã,¶ãƪã•«è¨˜è¼‰ã••ã,Œã•Ÿè„†å¼±æ€§ã•«å¯¾å‡¦ã•™ã,‹[ç„¡

ã

ï¿½Šå®¢æ§˜ã•Œã‚„ã‚µãƒãƒ¼ãƒˆã‚µãƒ¼ãƒ“ã‚¹ã‚„ãƒ‰ã‚ãƒ¥ãƒ¡ãƒ³ãƒˆã‚’å—ã‘å–ã‚‹ã•ã‚§ã‚¢ãƒ©ãƒ¼ãƒˆã‚µãƒ¼ãƒ“ã‚¹ã‚’ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ãƒ¼ã•ã‚“ã«æ¯Žæœˆé…ä¿¡ã™ã‚‹ã‚ˆã†ã«è¨å®šã—ã¦ã„ã‚‹å ´åˆã€ã¾ãŸã¯ã‚·ã‚¹ã‚³ã•ã‚“ã‚„ã‚·ã‚¹ã‚³ã®ãƒ‘ãƒ¼ãƒˆãƒŠãƒ¼ã•ã‚“ãŒã€ã‚·ã‚¹ã‚³ã®ã‚µãƒãƒ¼ãƒˆå¥‘ç´„ã‚’ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ãƒ¼ã•ã‚“ã«ä»£ã‚ã£ã¦ç®¡ç†ã™ã‚‹å ´åˆã€ã‚·ã‚¹ã‚³ã®ã‚µãƒãƒ¼ãƒˆå¥‘ç´„ã‚’ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ãƒ¼ã•ã‚“ã«ä»£ã‚ã£ã¦è¿½åŠ ã€ã¾ãŸã¯å¤‰æ›´ã™ã‚‹å ´åˆã€ã‚·ã‚¹ã‚³ã®ã‚µãƒãƒ¼ãƒˆå¥‘ç´„ã‚’ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ãƒ¼ã•ã‚“ã«ä»£ã‚ã£ã¦å‰Šé™¤ã™ã‚‹å ´åˆã€ã‚·ã‚¹ã‚³ã®ã‚µãƒãƒ¼ãƒˆå¥‘ç´„ã‚’ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ãƒ¼ã•ã‚“ã«ä»£ã‚ã£ã¦æ–°è¦ã«è¿½åŠ ã™ã‚‹å ´åˆ

Cisco ASA ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã•Ÿæœ€å^•ã•®ãƒªãƒªãƒ¼ã,¹ï¼‰
9.15 ä»¥å‰• [1]	è„†å¼±æ€§ã•ªã•—
9.16	9.16.3.19
9.17	9.17.1.13
9.18	9.18.2

1. Cisco ASA
ãƒ‡ãƒ•ã,¤ã,¹ã•Œè„†å¼±æ€§ã•®ã•,ã,‹ãƒªãƒªãƒ¼ã,¹ã•«ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã••ã,Œã•¦ã•‹ã,
9.16.1 ã•«ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã••ã,Œã•¦ã•‹ã,‰ãƒªãƒªãƒ¼ã,¹ 9.14.3.18
ã•«ãƒ€ã,¦ãƒ³ã,°ãƒ¬ãƒ¼ãƒ‰ã••ã,Œã•Ÿå ´å•ˆï¼‰ã€•è„†å¼±æ€§ã•®ã•ªã•„ãƒªãƒªãƒ¼ã,¹ã•®
RSA
ã,ãƒ¼ã•¯ã€•è„†å¼±æ€§ã•®ã•,ã,‹ãƒªãƒªãƒ¼ã,¹ã•«ä¿•å˜ã••ã,Œã•¦ã•„ã,‹ã•Ÿã,•ã€•ä¸•æ£ã
ASA
ãƒ‡ãƒ•ã,¤ã,¹ã•Œã•“ã•®æ–¹æ³•ã•§ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã•Šã,^ã•³ãƒ€ã,¦ãƒ³ã,°ãƒ¬ãƒ¼ãƒ‰ã•
ã,ãƒ¼ã•Œæœ‰åŠ¹ã•§ã•,ã,‹ã•“ã•¨ã,’ç¢ºèª•ã•—ã•¦ã••ã• ã••ã•„ã€,

FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

Cisco FTD ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒªãƒªãƒ¼ã,¹	First Fixed Releaseï¼ˆä¿®æ£ã•ã,Œã•Ÿæœ€å^•ã•®ãƒªãƒªãƒ¼ã,¹ï¼‰
6.7.0 ä»¥å‰• [1]	è„†å¼±æ€§ã•ªã•—
7.0.0	7.0.4
7.1.0	Cisco_FTD_Hotfix_P-7.1.0.2-2.sh.RE L.tar Cisco_FTD_SSP_FP1K_Hotfix_P-7.1.0.2-2.sh.RE L.tar Cisco_FTD_SSP_FP2K_Hotfix_P-7.1.0.2-2.sh.RE L.tar Cisco_FTD_SSP_Hotfix_P-7.1.0.2-2.sh.RE L.tar Cisco_FTD_SSP_FP3K_Hotfix_Q-7.1.0.3-2.sh.RE L.tar
7.2.0	7.2.0.1

1. Cisco FTD
ãƒ‡ãƒ•ã,¤ã,¹ã•Œè„†å¼±æ€§ã•®ã•,ã,‹ãƒªãƒªãƒ¼ã,¹ã•«ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã••ã,Œã•¦ã•‹ã,
7.0.0 ã•«ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã••ã,Œã•¦ã•‹ã,‰ãƒªãƒªãƒ¼ã,¹ 6.4.0.15
ã•«ãƒ€ã,¦ãƒ³ã,°ãƒ¬ãƒ¼ãƒ‰ã••ã,Œã•Ÿå ´å•ˆï¼‰ã€•è„†å¼±æ€§ã•®ã•ªã•„ãƒªãƒªãƒ¼ã,¹ã•®
RSA
ã,ãƒ¼ã•¯ã€•è„†å¼±æ€§ã•®ã•,ã,‹ãƒªãƒªãƒ¼ã,¹ã•«ä¿•å˜ã••ã,Œã•¦ã•„ã,‹ã•Ÿã,•ã€•ä¸•æ£ã
FTD
ãƒ‡ãƒ•ã,¤ã,¹ã•Œã•“ã•®æ–¹æ³•ã•§ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã•Šã,^ã•³ãƒ€ã,¦ãƒ³ã,°ãƒ¬ãƒ¼ãƒ‰ã•
ã,ãƒ¼ã•Œæœ‰åŠ¹ã•§ã•,ã,‹ã•“ã•¨ã,’ç¢ºèª•ã•—ã•¦ã••ã• ã••ã•„ã€,

Cisco FTD
ãƒ‡ãƒ•ã,¤ã,¹ã•®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰æ‰‹é †ã•«ã•¤ã•„ã•¦ã•¯ã€•ã€ŒCisco Firepower Management Center Upgrade Guideã€•ã,'å•,ç…§ã•—ã•¦ã••ã• ã••ã•„ã€,

æ³¨ï¼šä¿®æ£æ¸ˆã•¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ãƒªãƒªãƒ¼ã,¹ã•¸ã•®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰æ™‚ã•«ä¾µå®³ã

Product Security Incident Response Teamï¼^PSIRT; ãƒ—ãƒ€ã,¯ãƒˆ ã,»ã,ãƒ¥ãƒªãƒ†ã,£
ã,¤ãƒ³ã,·ãƒ‡ãƒ³ãƒˆ ãƒ¬ã,¹ãƒ•ãƒ³ã,¹
ãƒ•ãƒ¼ãƒ ï¼‰ã•¯ã€•ã•“ã•®ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã•«è¨˜è¼‰ã••ã,Œã•¦ã•„ã,‹è©²å½“ã•™ã

ä¸•æ£å^©ç”¨ä°‹ä¾‹ã•¨å…¬å¼•ç™ºè¡¨

Cisco PSIRT
ã•§ã•¯ã€•æœ¬ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã•«è¨˜è¼‰ã••ã,Œã•¦ã•„ã,‹è„†å¼±æ€§ã•®å…¬è¡¨ã,'ç¢º

ã•“ã•®ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã•§è¤‡æ•°ã••ã,Œã•¦ã•„ã,‹è„†å¼±æ€§ã•®æ,ªç”¨ã•«é–¢ã•™ã,‹æ
Cisco PSIRT ã•«å¯„ã•›ã,‰ã,Œã•¦ã•„ã•¾ã•›ã,“ã€,

å‡ºå…¸

ã•“ã•®è„†å¼±æ€§ã,'å ±å'Šã•—ã•¦ã•„ã•Ÿã• ã•„ã•Ÿã€•ã,«ãƒªãƒ•ã,©ãƒ«ãƒ‹ã,¢å¤§å¦ã,µãƒ³ãƒ‡
Nadia Heninger æ°•ã•¨ George Sullivan
æ°•ã€•ã,³ãƒãƒ©ãƒ‰å¤§å¦ãƒœãƒ€ãƒ¼æ ¡ã•® Jackson Sippe æ°•ã•¨ Eric Wustrow
æ°•ã•«æ„Ÿè¬•ã•„ã•Ÿã•—ã•¾ã•™ã€,

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz

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	å^•å›žå…¬é–‹ãƒªãƒªãƒ¼ã,¹	-	Final	2022 å¹´ 8 æœˆ 10 æ—¥

å^©ç”¨è¦•ç´„

æœ¬ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã•¯ç„¡ä¿è¨¼ã•®ã,,ã•®ã•¨ã•—ã•¦ã•”æ••ä¾›ã•—ã•¦ã•Šã,Šã€
æœ¬ã,¢ãƒ‰ãƒã,¤ã,¶ãƒªã•®æƒ…å ±ã•Šã,^ã•³ãƒªãƒ³ã,¯ã•®ä½¿ç”¨ã•«é–¢ã•™ã,‹è¬»ä»»ã•®ä¸€
ã•¾ã•Ÿã€•ã,·ã,¹ã,³ã•¯æœ¬ãƒ‰ã,ãƒ¥ãƒ¡ãƒ³ãƒˆã•®å†…å®¹ã,'ä°^å'Šã•ªã•—ã•«å¤‰æ›´ã•—ã•
æœ¬ã,¢ãƒ‰ãƒã

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—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

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。