ã‚·ã‚¹ã‚³è£½å“�ã�§ã�®Dual_EC_DRBGã�®ä½¿ç

Informational

ã‚¢ãƒ‰ãƒ�ã‚¤ã‚¶ãƒªãƒ¼ID : cisco-sa-20131016-ec-drbg

åˆ�å…¬é–‹æ—¥ : 2013-10-16 16:00

ãƒ�ãƒ¼ã‚¸ãƒ§ãƒ³ 1.0 : Final

å›žé�¿ç– : No Workarounds available

Cisco ãƒ�ã‚° ID :

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

æ¦‚è¦�

ã‚·ã‚¹ã‚³ã�¯ã€�Dual Elliptic Curve Deterministic Random Bit Generator(Dual_EC_DRBG)ã�«é–¢ã�™ã‚‹æ¥ç•Œã�®è°è«–ã�¨ã€�800-90A Special Publication(SP)ã‚’å†�ã‚ªãƒ¼ãƒ—ãƒ³ã�—ã�¦ä¸€èˆ¬ã�«å…¬é–‹ã�™ã‚‹ã�¨ã�„ã�†ç±³å›½å›½ç«‹æ¨™

ã‚·ã‚¹ã‚³ã�¯ã€�ã�“ã�®æ±ºå®šã�Œæš—å�·è¦�æ ¼ã�®å…¬é–‹å¯©æŸ»ã�®å¼·åŒ–ã�«ã�¤ã
SP 800-90Aã�®ã‚¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã‚’ç›£è¦–ã�—ã�¾ã�™ã€‚

ã‚·ã‚¹ã‚³ã�¯å†…éƒ¨èª¿æŸ»ã‚’å®Œäº†ã�—ã€�Dual_EC_DRBGã�Œã‚·ã‚¹ã‚³è£½å“�ã�§ä½¿ç”¨ã�•ã‚Œ

è¿½åŠ æƒ…å ±

ã‚·ã‚¹ã‚³ã�¯ã€�Dual_EC_DRBGã‚’å�«ã‚€ã‚µãƒ¼ãƒ‰ãƒ‘ãƒ¼ãƒ†ã‚£ãƒ³ãƒ�ãƒ¼ãƒ�ãƒ³ãƒˆã‚’ãƒ©ã‚¤ã‚»ã
Random Bit Generator(DRBG)ã�¯ã€�ã‚·ã‚¹ã‚³è£½å“�ã�§ã�¯ä½¿ç”¨ã�•ã‚Œã�¦ã�„ã�¾ã�›ã‚“ã€‚

æš—å�·åŒ–ã�«DRBGã‚’ä½¿ç”¨ã�™ã‚‹ã‚·ã‚¹ã‚³è£½å“�ã�¯ã€�å�¤ã�„ANSI X9.31è¦�æ ¼ã�¾ã�Ÿã�¯æ–°ã�—ã�„NIST SP 800-90Aè¦�æ ¼ã�«æº–æ‹ ã�—ã�¦ã�„ã�¾ã�™ã€‚ã‚·ã‚¹ã‚³è£½å“�ã�®800-90Aæº–æ‹ ã�®æš—å�·åŒ–ãƒ©ã‚¤ãƒ–ãƒ©ãƒªã�«ã�¯ã€�ã‚·ã‚¹ã‚³ã�®é–‹ç™ºè€…ã�Œä½¿ç”¨ã�§ã
Encryption Standard Counter(AES-CTR)ãƒ¢ãƒ¼ãƒ‰ã�§ã�™ã€‚ã�¾ã�Ÿã€�Dual_EC_DRBGã‚’æœ‰åŠ¹ã�«ã�™ã‚‹è¨å®šå¤‰æ›´ã�¯

ã,·ã,¹ã,³ã�¯ã€�å›½éš›è¦�æ ¼ã,„å�„å›½ã�®è¦�åˆ¶ã�«æº–æ‹ ã�—ã�Ÿå¼·åŠ›ã�ªæš—å�·åŒ–ã

ã,·ã,¹ã,³ã�®ã,»ã,ãƒ¥ãƒªãƒ†ã,£æ‰‹é †

ã,·ã,¹ã,³è£½å“�ã�«ã�Šã�'ã,‹ã,»ã,ãƒ¥ãƒªãƒ†ã,£ã�®è„†å¼±æ€§ã�®å ±å'Šã€�ã,»ã,ãƒ¥ãƒªãƒ†ã,£ä º‹æ
ttps://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html
ã�«ã�,ã,‹ã,·ã,¹ã,³ã�®ãƒ¯ãƒ¼ãƒ«ãƒ‰ãƒ¯ã,¤ãƒ‰Webã,µã,¤ãƒˆã,'å�,ç…§ã�—ã�¦ã���ã� ã�•ã�„ã
Cisco ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã�¯ã€�http://www.cisco.com/go/psirt
ã�‹ã,‰å…¥æ‰‹ã�§ã���ã�¾ã�™ã€,

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131016-ec-drbg

æ”¹è¨‚å±¥æ´

ãƒ�ãƒ¼ã,¸ãƒ§ãƒ³	èª¬æ˜Ž	ã,»ã,¯ã,·ãƒ§ãƒ³	æ—¥ä»˜
ãƒªãƒ"ã,¸ãƒ§ãƒ³ 1.0	åˆ�å›žå…¬é–‹ãƒªãƒªãƒ¼ã,¹		2013å¹´10æœˆ16æ—¥

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