REPORT NESSUS

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness - CVE-2008-0166

- The remote SSH host keys are weak.
  "La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
  Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.
  Un attaccante potrebbe facilmente ottenere la parte privata della chiave remota e sfruttarla per decifrare la sessione remota o eseguire attacchi man-in-the-middle."

soluzione report: Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL, and OpenVPN key material should be re-generated.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL Check) - CVE-2008-0166

- The remote SSL certificate uses a weak key.
  "Il certificato x509 remoto sul server SSL è stato generato su un sistema Debian o Ubuntu affetto da un bug nel generatore di numeri casuali della libreria OpenSSL.
  Il problema deriva da una modifica apportata da un maintainer Debian, che ha eliminato quasi tutte le fonti di entropia nella versione remota di OpenSSL.
  Un attaccante può facilmente ottenere la chiave privata corrispondente e usarla per decifrare la sessione remota o condurre un attacco man-in-the-middle."

soluzione report: Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL, and OpenVPN key material should be re-generated.

20007 - SSL Version 2 and 3 Protocol Detection

- The remote service encrypts traffic using a protocol with known weaknesses.
  *"Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni presentano diverse vulnerabilità, tra cui:

Uno schema di padding non sicuro con cifrari CBC.
Schemi di negoziazione e ripresa delle sessioni insicuri.
Un attaccante può sfruttare queste debolezze per eseguire attacchi man-in-the-middle o decifrare comunicazioni tra il servizio e i client.
Nonostante SSL/TLS offra un meccanismo per selezionare la versione più sicura, molti browser lo

implementano in modo errato, consentendo il downgrade della connessione (es. POODLE). Disabilitare completamente questi protocolli è altamente raccomandato.*

soluzione report: Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) - CVE-2016-2183

- The remote service supports the use of medium strength SSL ciphers.
  "L'host remoto supporta cifrature SSL che offrono una crittografia di forza media.
  Nessus considera tali cifrature con chiavi di lunghezza tra 64 e 112 bit, o che utilizzano la suite di cifratura 3DES.
  Un attaccante sulla stessa rete fisica può aggirare più facilmente la crittografia di forza media."

soluzione report: Reconfigure the affected application if possible to avoid use of medium strength ciphers.

90509 - Samba Badlock Vulnerability - CVE-2016-2118

- An SMB server running on the remote host is affected by the Badlock vulnerability.
  "La versione di Samba in esecuzione sull'host remoto è vulnerabile al problema Badlock, che colpisce i protocolli SAM e LSAD.
  Un attaccante man-in-the-middle potrebbe forzare un downgrade del livello di autenticazione, consentendogli di eseguire operazioni arbitrarie, come modificare dati sensibili in Active Directory o disabilitare servizi critici."

soluzione report: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

11213 - HTTP TRACE / TRACK Methods Allowed

- Debugging functions are enabled on the remote web server.
  "Il server web remoto supporta i metodi HTTP TRACE e TRACK, utilizzati per il debug delle connessioni. Questi metodi possono rappresentare un rischio per la sicurezza."

Disable these HTTP methods. Refer to the plugin output for more information.

#57608 - SMB Signing not required

- Signing is not required on the remote SMB server.
  "La firma non è obbligatoria sul server SMB remoto. Ciò consente a un attaccante non autenticato di eseguire attacchi man-in-the-middle contro il server SMB."

soluzione report: Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting

is called 'server signing'.