Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.

Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle.

Solution

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

Soluzione

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

- No output recorded.

Critical: rlogin Service Detection

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.
Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Descrizione

Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono passati tra il client e il server rlogin in chiaro. Un utente malintenzionato man-in-the-middle può sfruttare questa situazione per sniffare login e password. Inoltre, potrebbe consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su una rete locale), potrebbe essere possibile ignorare l'autenticazione.
Infine, rlogin è un modo semplice per trasformare l'accesso in scrittura su file in accessi completi tramite i file .rhosts o rhosts.equiv.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Soluzione

Commentare la riga 'login' in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilita questo servizio e utilizza invece SSH.