

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Soluzione

Abilita il supporto per TLS 1.2 e 1.3 e disabilita il supporto per TLS 1.0.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Output

- TLSv1 is enabled and the server supports at least one cipher.

Medium: Unencrypted Telnet Server.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Descrizione

L'host remoto esegue un server Telnet su un canale non crittografato.

Non è consigliabile utilizzare Telnet su un canale non crittografato poiché login, password e comandi vengono trasferiti in chiaro. Ciò consente a un utente malintenzionato remoto, man-in-the-middle, di intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e modificare il traffico scambiato tra un client e un server.

SSH è preferito a Telnet poiché protegge le credenziali dalle intercettazioni e può eseguire il tunneling di flussi di dati aggiuntivi come una sessione X11.

Soluzione

Disattiva il servizio Telnet e utilizza invece SSH.

Output

- Nessus collected the following banner from the remote Telnet server :

----- snip -----