Solution

Place the appropriate restrictions on all NFS shares.

Soluzione

Posizionare le opportune restrizioni su tutte le condivisioni NFS.

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Output

- The following shares have no access restrictions :

  / *

-Vulnerabilita meno critiche trovata nello scan a metasploitablet 2

Medium: TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando TLS 1.0. TLS 1.0 presenta numerosi difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 mitigano questi problemi, ma le versioni più recenti di TLS come 1.2 e 1.3 sono progettate contro questi difetti e dovrebbero essere utilizzate quando possibile.

A partire dal 31 marzo 2020, gli endpoint che non sono abilitati per TLS 1.2 e versioni successive non funzioneranno più correttamente con i principali browser Web e i principali fornitori.

PCI DSS v3.2 richiede che TLS 1.0 sia completamente disabilitato entro il 30 giugno 2018, ad eccezione dei terminali POS POI (e dei punti terminali SSL/TLS a cui si connettono) che possono essere verificati come non suscettibili ad eventuali exploit noti.