REPORT VULNERABILITA' METASPLOITABLE

NOME VULNERABILITA': NFS Shares World Readable

DESCRIZIONE: Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP, o intervallo IP).

SOLUZIONE: Applicare le restrizioni appropriate su tutte le condivisioni NFS.

FATTORE DI RISCHIO: ALTO

PLUGIN OUTPUT: tcp/2049/rpc-nfs

NOME VULNERABILITA': SSL Medium Strenght Cipher Suites Supported (SWEET32)

DESCRIZIONE: L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio. Nessus applica questo livello a qualsiasi crittografia che utilizzi lunghezze di chiave da 64 a 112 bit, oppure che utilizza la crittografia 3DES.

Se l'attaccante si trova sulla stessa rete è molto più semplice aggirare questo tipo di crittografia.

SOLUZIONE: Riconfigurare l'application in modo da evitare questo tipo di cifratura.

FATTORE DI RISCHIO: ALTO

PLUGIN OUTPUT: tcp/25/smtp & tcp/5432/postgresql

NOME VULNERABILITA': Samba Badlock Vulnerability

DESCRIZIONE: La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto ha un difetto, chiamato Badlock, che si trova nel Security Account Manager (che è un file di database di Windows che memorizza le password degli utenti) e nei protocolli di Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione errata del livello di autenticazione su chiamata di procedura remota (RPC). Un attaccante man-in-the-middle che è in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questo difetto per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati di sicurezza sensibili nel database di Active Directory (AD) o la disabilitazione di servizi critici.

SOLUZIONE: Aggiornare Samba alla versione 4.2.11 o superiore.

FATTORE DI RISCHIO: ALTO

PLUGIN OUTPUT: tcp/445/cifs