REPORT TECNICO VULNERABILITA DI LIVELLO ALTO

- **136769 - Downgrade del servizio ISC BIND / DoS riflesso – 8.6 Score**

Descrizione:

Secondo la sua versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è affetta da vulnerabilità di downgrade delle prestazioni e DoS riflesso. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di fetch che possono essere eseguiti durante l'elaborazione di una risposta di rinvio.
Un aggressore remoto non autenticato può sfruttare questa situazione per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come un server riflesso. Utilizzare il server interessato come riflettore in un attacco di riflessione.

Soluzione:

Aggiornare alla versione di ISC BIND indicata nell'avviso del fornitore. Versione Installata : **9.4.2** – Versione Fixata : **9.11.19**

- **42256 - Condivisioni NFS leggibili in tutto il mondo - 7.5 Score**

Descrizione

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

Soluzione:

Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

- **42873 - Suite di cifratura SSL a media resistenza supportate (SWEET32) - 7.5 score**

Descrizione:

L'host remoto supporta l'uso di cifrari SSL che offrono una crittografia di media forza. Nessus considera media forza qualsiasi crittografia che utilizzi chiavi di lunghezza pari ad almeno 64 bit e inferiore a 112 bit, oppure che utilizza la suite di crittografia 3DES.
Si noti che è molto più facile aggirare la crittografia a media resistenza se l'aggressore si trova sulla stessa rete fisica.

Soluzione:

Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di cifrari di media potenza.