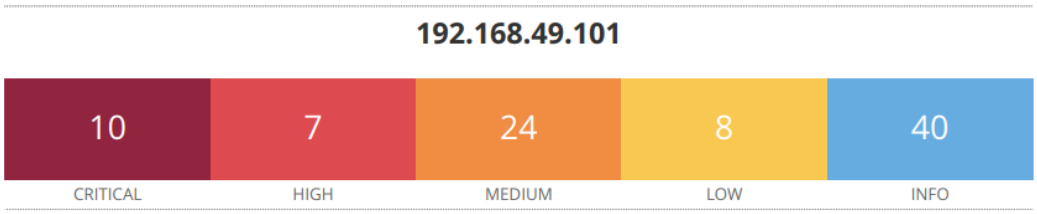
Tenable Nessus

Dopo aver effettuato la scansione attraverso l'applicativo Tenable Nessus sono state trovate diverse problematiche, andiamo a vederle piu' nel dettaglio



le criticità "critical"

- Il server web remoto contiene una versione di PHP che consente l'esecuzione di codice arbitrario.

Descrizione:

L'installazione di PHP sul server web remoto contiene un difetto che potrebbe consentire a un utente malintenzionato remoto di passare argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Se ne potrebbe abusare per eseguire codice arbitrario, rivelare il codice sorgente PHP, causare un arresto anomalo del sistema, ecc.

Soluzione

Aggiorna a PHP 5.3.13 / 5.4.3 o versioni successive.

- È presente un connettore AJP vulnerabile in ascolto sull'host remoto.

Descrizione:

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice in modalità remota (RCE).

Soluzione:

Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

- L'host remoto potrebbe essere stato compromesso.

Descrizione:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione:

Verifica se l'host remoto è stato compromesso e, se necessario, reinstalla il sistema.

- Il servizio remoto crittografa il traffico utilizzando un protocollo con punti deboli noti.

Descrizione:

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:
- Uno schema di riempimento non sicuro con cifrari CBC.
- Schemi di rinegoziazione e ripresa delle sessioni non sicuri.
Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client.

Soluzione

Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0. Utilizza invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

- Il server Web remoto ospita un'applicazione PHP interessata dalla vulnerabilità SQLi.

Descrizione:

Secondo il numero di versione riportato, l'applicazione phpMyAdmin ospitata sul server web remoto è precedente alla 4.8.6. È quindi affetto da una vulnerabilità SQL injection (SQLi) presente nella funzionalità di progettazione di phpMyAdmin. Un utente malintenzionato remoto non autenticato può sfruttare questa situazione per inserire o manipolare query SQL nel database back-end, con conseguente divulgazione o manipolazione di dati arbitrari.

Soluzione:

Aggiorna a phpMyAdmin versione 4.8.6 o successiva.

- Il sistema operativo in esecuzione sull'host remoto non è più supportato.

Descrizione:

Secondo il numero di versione riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

Soluzione:

Esegui l'upgrade a una versione del sistema operativo Unix.

- Le chiavi dell'host SSH remoto sono deboli.

Descrizione

La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.

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.

- È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione:

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

Soluzione:

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano accedere alle condivisioni.

- Il server dei nomi remoto è interessato da vulnerabilità di downgrade del servizio/DoS riflesse.

Descrizione:

Secondo la versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto al fatto che BIND DNS non limita sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.

Soluzione:

Aggiorna alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore.