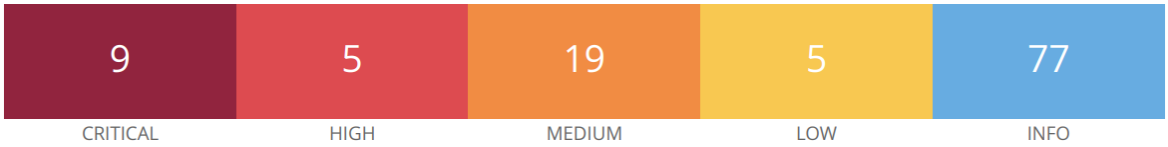
Scansione vulnerabilità indirizzo 192.168.30.200

Data: 2-22-2023
14:32 - 14:35



Il sistema presenta in totale 115 vulnerabilità, l' immagine sopra descrive la divisione di queste in base al loro grado di pericolosità.
Quelle di livello più alto (da medio in su) vanno risolte in tempi brevi per evitare un'esposizione eccessiva agli attacchi da parte di malintenzionati.

Descrizione ed eventuale soluzione alle principali vulnerabilità:

CRITICAL Un AJP vulnerabile è in ascolto su l'host remoto, questo potrebbe permettere ad un attaccante di leggere file da applicazioni web, e in questo caso pure di iniettare codice di pagine JS malevole da remoto.
RISOLUZIONE: aggiornare i sistemi e apportare una giusta configurazione al server Tomcat.

CRITICAL Una shell è in ascolto sulla porta remota senza alcuna autenticazione, un attaccante potrebbe connettersi alla porta e inviare comandi da remoto.
RISOLUZIONE: verificare se l'host remoto è stato compromesso e in caso reinstallare il sistema.

CRITICAL Il servizio remoto che usa SSL v.2/3 non è sicuro dato che questi protocolli hanno delle debolezze conosciute, un attaccante che effettua un attacco man in the middle sulle comunicazioni criptate con questi protocolli può tranquillamente decifrare i dati mettendo a rischio la sicurezza degli stessi.
RISOLUZIONE: evitare di usare sistemi deprecati ed aggiornarsi a sistemi come TLS 1.2 o supreriori.

CRITICAL Il sistema operativo della macchina non è più supportato quindi non ricevendo aggiornamenti rimane vulnerabile a qualsiasi nuovo exploit trovato.
RISOLUZIONE: aggiornare i sistemi ad una versione supportata.

CRITICAL Le chiavi dell'host SSH sono deboli e facilmente ottenibili da un attaccante per colpa di una libreria Debian contenente bug.
RISOLUZIONE: rigenerare tutte le chiavi dei protocolli SSH, SSL e OpenVPN.

CRITICAL Il sistema che consente a computer client di utilizzare la rete per accedere a directory condivise da server remoti non ha sistemi di sicurezza ed un attaccante potrebbe accedere per leggere e scrivere file.
RISOLUZIONE: configurare NFS sull'host remoto autorizzando solo le fonti certe.

CRITICAL Il sistema di desktop-sharing è protetto da una password debole "password".
RISOLUZIONE: cambiare password mettendo almeno 12 caratteri una lettera maiuscola e un carattere speciale.

CRITICAL Il servizio di esecuzione di comandi remoti rexecd è attivo sul demone di reindirizzamento delle chiamate TCP e UDP del sistema ma senza assicurare nessun livello di protezione ed un attaccante potrebbe usarlo per scansionare la rete.
RISOLUZIONE: configurare correttamente il demone inetd abbattendo il servizio.

HIGH La versione di ISC BIND installata nel sistema è obsoleta e un attaccante potrebbe facilmente fare un attacco di tipo Reflected DoS o Service Downgrade causando ingenti danni al sistema.
RISOLUZIONE: aggiornare l'istanza del servizio seguendo le norme del fornitore.

HIGH Il Network File System esporta uno o più condivisioni senza applicare livelli di sicurezza.
RISOLUZIONE: configurare correttamente apportando le giuste restrizioni a tutte le condivisioni.

HIGH Il servizio remoto utilizza un protocollo di criptazione di media sicurezza facilmente attaccabile se ci si trova nella stessa rete fisica.
RISOLUZIONE: riconfigurare tutte le applicazioni che lo utilizzano ed evitare di riusarlo in futuro passando ad un algoritmo più sicuro.

HIGH Il server SMB che gira sull host remoto ha una vulnerabilità di tipo Badlock, un attaccante potrebbe intercettare le comunicazioni in chiaro dall host al database.
RISOLUZIONE: aggiornare a Samba v.4.3 o superiori.

HIGH Il servizio rlogin gira sull host remoto, quindi i dati passano in chiaro dal servizio di login al server ed un attaccante li può intercettare senza problemi.
RISOLUZIONE: disabilitare il servizio ed usare SSH.

MEDIUM C'è la possibilità da parte di un attaccante di accedere a informazioni riservate dell host dal servizio SSL v.3.
RISOLUZIONE: disabilitare il servizio o se non possibile abilitare il meccanismoTLS Fallback SCSV.

MEDIUM La versione di BIND è obsoleta ed espone la macchina ad attacchi di tipo DoS.
RISOLUZIONE: aggiornare il servizio alla versione 9.16 o successive.

MEDIUM Il servizio SSL è obsoleto.
RISOLUZIONE: comprare o generare un nuovo certificato SSL.

MEDIUM Funzioni di debug accessibili dal web server.
RISOLUZIONE: disabilitare i metodi HTTP Trace e Track.

CONCLUSIONI:

Se applicate tutte le risoluzioni consigliate anche quelle meno pericolose dovrebbero risolversi di conseguenza, importante applicare nel breve periodo risoluzioni almeno alle criticità maggiori indicate come critiche e alte successivamente quelle medie.

Le vulnerabilità di tipo info e basso che non verranno risolte a cascata dalle correzioni di quelle più pericolose possono essere momentaneamente tralasciate ma bisogna avere la consapevolezza che un attaccante potrebbe usarle per ottenere maggiori informazioni sulla macchina, di conseguenza rendere più facile l'intrusione nel sistema.
