Nella scansione dell'host richiesto sono stare individuate 11 vulnerabilità critiche che necessitano un'azione immediata per evitare eventuali attacchi ed altre 5 vulnerabilità a rischio alto che vanno anch'esse eliminate successivamente.

Vulnerabilities Total: 108

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	-	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability

- La prima vulnerabilità di lettura/inclusione nel connettore AJP, dove un attaccante 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 il codice JavaServer Pages (JSP) e ottenere l'esecuzione di codice remoto (RCE). La soluzione consigliata sarebbe quella di aggiornare la configurazione di APJ e aggiornare il server Tomcat a una versione 9.0.31 o successiva.

- La seconda vulnerabilità riguarda la possibile compromissione dell'host remoto tramite una shell in ascolto su una porta remota senza alcuna autorizzazione, la soluzione richiede di verificare un eventuale compromissione e reinstallare il sistema se necessario.

- Abbiamo poi tre vulnerabilità critiche riguardanti le chiavi dell'host SSH remoto deboli. 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. Il problema è dovuto al fatto che un packager Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the middle. Quindi dobbiamo considerare tutto il materiale crittografico generato sull'host remoto facilmente accessibile da un eventuale malintenzionato, in particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

- La sesta vulnerabilità riguarda il remote name resolver (o il server che utilizza a monte) è interessato da una vulnerabilità di avvelenamento della cache DNS. Il remote DNS resolver non utilizza porte casuali quando esegue una richiesta su server DNS di terze parti. Un utente malintenzionato remoto non autenticato può sfruttare questa situazione per avvelenare il server DNS remoto, consentendogli di deviare il traffico legittimo

verso siti arbitrari, bisogna quindi contattare il fornitore del server DNS per un aggiornamento di sicurezza che risolva il bug.

- La settima vulnerabilità è dovuta al fatto che è possibile accedere alle condivisioni NFS sull'host remoto. Almeno una delle condivisioni NFS esportate dal server potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) un file sull'host remoto. Per risolvere questa vulnerabilità bisogna configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

- Abbiamo poi due vulnerabilità causate dalla crittografia usata su una risorsa remota che utilizza un protocollo con punti deboli noti. 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 clienti.
  Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più alta supportata del protocollo (queste versioni verranno utilizzate solo se il client o il server non supportano niente di meglio), molti browser web lo implementano in un modo non sicuro che consente a un utente malintenzionato di eseguire il downgrade di una connessione (come in POODLE).
  Pertanto, si consiglia di disattivare completamente questi protocolli.
  Il NIST "National Institute of Standards and Technology" ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. La soluzione è quella di consultare la documentazione del servizio per disattivare SSL 2.0 e 3.0 ed utilizzare invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

- La decima vulnerabilità con rischio 10 è causata dal sistema operativo in esecuzione sull'host remoto che non è più supportato. Il numero di versione del sistema operativo Unix in esecuzione sull'host remoto non è più supportato; la mancanza di supporto implica che il fornitore non rilascerà alcuna nuova patch di sicurezza per il prodotto e di conseguenza, è probabile che contenga vulnerabilità di sicurezza. Bisogna quindi eseguire l'upgrade a una versione del sistema operativo Unix attualmente supportata.

- L'undicesima vulnerabilità con rischio 10 è causata da un server VNC in esecuzione sull'host remoto protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema. La soluzione è quindi proteggere il servizio VNC con una password complessa.

Abbiamo poi 5 vulnerabilità a rischio alto che necessitano un intervento dopo aver risolto quelle critiche.

- La prima vulenrabilità ad alto 8,6 rischio riguarda il server dei nomi remoto DNS che è interessato da vulnerabilità di downgrade del servizio/DoS riflesso. 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 riflesso. 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. Un utente malintenzionato può sfruttare questa situazione per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione. La soluzione è aggiornare alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore

- La seconda e terza vulnerabilità a rischio alto 7,5 riguardano il servizio remoto che supporta l'uso di crittografie SSL di media potenza, l'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio (utilizza chiavi di lunghezza compresa tra almeno 64 bit e meno di 112 bit, oppure che utilizza la suite di crittografia 3DES). Bisogna considerare che è molto più semplice eludere la crittografia di livello

medio se l'aggressore si trova sulla stessa rete; per questo bisogna ,se possibile, riconfigurare l'applicazione interessata per evitare l'uso di crittografie di media complessità.

- La quarta vulnerabilità ad alto rischio 7,5 è causata da un server SMB in esecuzione sull'host remoto che è interessato dalla vulnerabilità Badlock. La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come **Badlock**, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici. È quindi necessario aggiornare Samba ad una versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.

- La quinta è dovuta al server NFS remoto che esporta condivisioni leggibili da tutto il mondo; questo sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP, o intervallo IP). Si devono posizionare le opportune restrizioni su tutte le condivisioni NFS per risolvere la vulnerabilità.