ANALISI DELLE VULNERABILITÀ

CRITICAL VULNERABILITY

	DESCRIZIONE
Apache Tomcat A JP Connector Request Injection (Ghostcat)	Una vulnerabilità di lettura/inclusione del file è stata trovata in un connettore JP. Un 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 il codice JavaServer Pages (JSP) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).
Bind Shell Backdoor Detection	Una shell sta ascoltando sulla porta remota senza alcuna autenticazione richiesta. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.
SSL Version 2 and 3 Protocol Detection	SSL è acronimo di Secure Sockets Layer, un protocollo di sicurezza che crea un link crittografato fra un server web e un browser web.
Unix Operating System Unsupported Version Detection	Secondo il suo numero di versione, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato. La mancanza di supporto implica che nessuna nuova patch di sicurezza per il prodotto sarà rilasciato dal fornitore.
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Il certificato remoto x509 sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un uomo nell'attacco centrale.

NFS Exported Share Information Disclosure	Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato può essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) i file su host remoto.
VNC Server 'password' Password	Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di 'password'. Un attaccante remoto e non autenticato potrebbe sfruttarlo per prendere il controllo del sistema.

HIGH VULNERABILITY

	DESCRIZIONE
ISC BIND Service Downgrade / Reflected DoS	L'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è influenzata 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 rinvio. Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco riflesso.
ISC BIND Denial of Service	Una vulnerabilità denial of service (DoS) esiste nelle versioni BIND di ISC 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 e precedenti. Un non autenticato, attaccante remoto può sfruttare questo problema, tramite un messaggio appositamente predisposto, per causare il servizio di smettere di rispondere. Si noti che Nessus non ha testato per questo problema, ma ha invece fatto affidamento solo sul numero di versione auto-riferito dell'applicazione.
NFS Shares World Readable	Il server NFS remoto esporta una o più condivisioni senza limitare l'accesso (in base al

	nome host, all'IP o all'intervallo IP).
SSL Medium Strength Cipher Suites Supported (SWEET32)	Il server NFS remoto esporta una o più condivisioni senza limitare l'accesso (in base al nome host, all'IP o all'intervallo IP).
Samba Badlock Vulnerability	La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetto da un difetto, noto come Badlock. Un attaccante è 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.