REPORT TECNICO VULNERABILITY ASSESSMENT METASPLOITABLE

192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
8	3	14	4	102

Scan Information

Start time:	Thu Feb 23 09:15:46 2023
End time:	Thu Feb 23 09:47:55 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.101
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descrizione:

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Potrebbe farlo un utente malintenzionato remoto e non autenticato sfruttare questa vulnerabilità per leggere i file dell'applicazione 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 una varietà di tipi di file e ottenere l'esecuzione di codice remoto (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

51988 - Bind Shell Backdoor Detection

Descrizione:

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

Soluzione:

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Descrizione:

La chiave dell'host SSH remoto è stata generata su un sistema Debian o Ubuntu che contiene un bug nel file generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un packager Debian che rimuove 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 impostare la decifrazione del telecomando sessione o impostare un uomo nel mezzo dell'attacco.

Soluzione:

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH, Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Descrizione:

Il certificato x509 remoto 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. Il problema è dovuto a un packager Debian che rimuove 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 uomo nel mezzo dell'attacco.

Soluzione:

Considerare indovinabile tutto il materiale crittografico generato sull'host remoto. In particolare, tutti gli SSH, Il materiale delle chiavi SSL e OpenVPN deve essere rigenerato.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

(Come sopra)

11356 - NFS Exported Share Information Disclosure

Descrizione:

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. UN l'attaccante potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

Soluzione:

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

33850 - Unix Operating System Unsupported Version Detection

Descrizione:

Secondo il suo numero di versione auto-riportato, il sistema operativo Unix in esecuzione sull'host remoto è non più supportato. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Come un risultato, è probabile che contenga vulnerabilità di sicurezza.

Soluzione:

Aggiorna a una versione del sistema operativo Unix attualmente supportata.

61708 - VNC Server 'password' Password

Descrizione:

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password di 'password'. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

Soluzione:

Proteggi il servizio VNC con una password complessa.

136769 - ISC BIND Service Downgrade / Reflected DoS

Descrizione

Secondo la sua versione auto-segnalata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è influenzato dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto a BIND DNS no limitando 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 utilizzare il server interessato come riflettore in un attacco di riflessione.

Soluzione:

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

42256 - NFS Shares World Readable

Descrizione:

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

Soluzione:

Posizionare le restrizioni appropriate su tutte le condivisioni NFS.

90509 - Samba Badlock Vulnerability

Descrizione:

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è interessata da un difetto, noto come Badlock, che esiste nel Security Account Manager (SAM) e nell'autorità di sicurezza locale (Domain Policy) (LSAD) a causa di una negoziazione errata del livello di autenticazione su procedura remota Canali di chiamata (RPC). Un attaccante man-in-the-middle che è in grado di intercettare il traffico tra un client e un server che ospita un database SAM possono sfruttare questo difetto per forzare un downgrade dell'autenticazione livello, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati di sicurezza sensibili nel database di Active Directory (AD) o la disabilitazione servizi critici.

Soluzione:

Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

11213 - HTTP TRACE / TRACK Methods Allowed

Descrizione:

Il server Web remoto supporta i metodi TRACE e/o TRACK. TRACE e TRACK sono metodi http utilizzati per eseguire il debug delle connessioni del server Web.

Soluzione:

Disattiva questi metodi HTTP. Fare riferimento all'output del plug-in per ulteriori informazioni.

139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Descrizione

In base al numero di versione auto-riportato, l'installazione di ISC BIND in esecuzione sul nome remoto server è la versione 9.x precedente alla 9.11.22, 9.12.x precedente alla 9.16.6 o 9.17.x precedente alla 9.17.4. È, quindi, influenzato da una vulnerabilità di negazione del servizio (DoS) dovuta a un errore di asserzione durante il tentativo di verificare un file troncato risposta a una richiesta firmata da TSIG. Un utente malintenzionato remoto autenticato può sfruttare questo problema inviando un file risposta troncata a una richiesta firmata TSIG per attivare un errore di asserzione, causando l'uscita dal server. Si noti che Nessus non ha testato questo problema, ma si è invece affidato solo alle auto-segnalazioni dell'applicazione numero della versione.

Soluzione

Aggiorna a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.

136808 - ISC BIND Denial of Service

Descrizione:

Esiste una vulnerabilità Denial of Service (DoS) nelle versioni ISC BIND 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 utente malintenzionato remoto non autenticato può sfruttare questo problema, tramite un messaggio appositamente predisposto, per impedire al servizio di

rispondere. Si noti che Nessus non ha testato questo problema, ma si è invece affidato solo alle auto-segnalazioni dell'applicazione numero della versione.

Soluzione:

Aggiorna alla versione con patch più strettamente correlata alla tua attuale versione di BIND.

57608 - SMB Signing not required

Descrizione

La firma non è richiesta sul server SMB remoto. Un utente malintenzionato remoto non autenticato può sfruttarlo per condurre attacchi man-in-the-middle contro il server SMB.

Soluzione

Imponi la firma dei messaggi nella configurazione dell'host. Su Windows, questo si trova nell'impostazione dei criteri 'Server di rete Microsoft: firmare digitalmente le comunicazioni (sempre)'. Su Samba, l'impostazione si chiama 'server firma'. Vedere i collegamenti "vedi anche" per ulteriori dettagli.

52611 - SMTP Service STARTTLS Plaintext Command Injection

Descrizione:

Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire a utente malintenzionato remoto e non autenticato per iniettare comandi durante la fase del protocollo in chiaro che sarà eseguito durante la fase del protocollo del testo cifrato. Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o SASL (Simple credenziali di autenticazione e livello di sicurezza).

Soluzione:

Contattare il fornitore per vedere se è disponibile un aggiornamento.

90317 - SSH Weak Algorithms Supported

Descrizione:

Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario a flusso Arcfour o no cifrare affatto. RFC 4253 sconsiglia l'utilizzo di Arcfour a causa di un problema con chiavi deboli.

Soluzione:

Contattare il fornitore o consultare la documentazione del prodotto per rimuovere le cifrature deboli.

51192 - SSL Certificate Cannot Be Trusted

Descrizione:

Il certificato X.509 del server non può essere attendibile. Questa situazione può verificarsi in tre modi diversi, in cui la catena della fiducia può essere spezzata, come indicato di seguito:

- In primo luogo, la parte superiore della catena di certificati inviata dal server potrebbe non discendere da un pubblico noto autorità di certificazione. Ciò può verificarsi quando la parte superiore della catena è un'autofirmata non riconosciuta certificato o quando mancano certificati intermedi che collegherebbero la parte superiore della catena di certificati a un'autorità di certificazione pubblica nota.

- In secondo luogo, la catena di certificati potrebbe contenere un certificato non valido al momento della scansione. Questo può verificarsi quando la scansione avviene prima di una delle date 'notBefore' del certificato o dopo una delle date le date "notAfter" del certificato.

- In terzo luogo, la catena di certificati potrebbe contenere una firma che non corrispondeva alle informazioni del certificato o non è stato possibile verificarlo. Le firme errate possono essere corrette ottenendo il certificato con la firma errata nuovamente firmato dal suo emittente. Le firme che non è stato possibile verificare sono il risultato dell'utilizzo da parte dell'emittente del certificato a algoritmo di firma che Nessus non supporta o non riconosce.

Se l'host remoto è un host pubblico in produzione, qualsiasi interruzione nella catena rende le cose più difficili per gli utenti per verificare l'autenticità e l'identità del server web. Ciò potrebbe semplificare l'esecuzione di attacchi man-in-the-middle contro l'host remoto.

Soluzione:

Acquista o genera un certificato SSL appropriato per questo servizio.

51192 - SSL Certificate Cannot Be Trusted

(Come sopra)

15901 - SSL Certificate Expiry

Descrizione:

Questo plug-in controlla le date di scadenza dei certificati associati ai servizi abilitati SSL sulla destinazione e segnala se qualcuno è già scaduto.

Soluzione:

Acquista o genera un nuovo certificato SSL per sostituire quello esistente

15901 - SSL Certificate Expiry

(Come sopra)

45411 - SSL Certificate with Wrong Hostname

Descrizione:

L'attributo 'commonName' (CN) del certificato SSL presentato per questo servizio è per una macchina diversa.

Soluzione:

Acquista o genera un certificato SSL appropriato per questo servizio

45411 - SSL Certificate with Wrong Hostname

(Come sopra)

57582 - SSL Self-Signed Certificate

Descrizione:

La catena di certificati X.509 per questo servizio non è firmata da un'autorità di certificazione riconosciuta. Se il telecomando host è un host pubblico in produzione, questo annulla l'uso di SSL in quanto chiunque potrebbe stabilire un attacco man-in-the-middle contro l'host remoto. Si noti che questo plug-in non controlla le catene di certificati che terminano con un certificato non autofirmato, ma è firmato da un'autorità di certificazione non riconosciuta.

Soluzione:

Acquista o genera un certificato SSL appropriato per questo servizio.

57582 - SSL Self-Signed Certificate

(Come sopra)

REPORT DIRIGENZA VULNERABILITY ASSESSMENT METASPLOITABLE

192.168.50.101

7	3	10	4	56
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 80

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
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	90509	Samba Badlock Vulnerability
MEDIUM	6.5	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	57582	SSL Self-Signed Certificate
MEDIUM	5.9	136808	ISC BIND Denial of Service
MEDIUM	5.3	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	15901	SSL Certificate Expiry
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname

MEDIUM	4.0*	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	90317	SSH Weak Algorithms Supported
LOW	3.7	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	10407	X Server Detection
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	21186	AJP Connector Detection
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	84574	Backported Security Patch Detection (PHP)
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection

INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	10437	NFS Share Export List
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	118224	PostgreSQL STARTTLS Support
INFO	N/A	26024	PostgreSQL Server Detection
INFO	N/A	22227	RMI Registry Detection
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	53335	RPC portmapper (TCP)
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	42088	SMTP Service STARTTLS Command Support
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

INFO	N/A	22964	Service Detection
INFO	N/A	17975	Service Detection (GET request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	19288	VNC Server Security Type Detection
INFO	N/A	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	10342	VNC Software Detection
INFO	N/A	135860	WMI Not Available
INFO	N/A	11424	WebDAV Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown