Nessus Essentials

mestploi

Report generated by Nessus™ Wed, 10 May 2023 18:23:11 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

192.168.49.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	3	3	1	80

Scan Information

Start time:	Wed May 10 18:13:56 2023
End time:	Wed May 10 18:23:11 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.49.101
MAC Address:	08:00:27:B1:AA:58
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

Vulnerabilities

Considerazioni generali

Dai risultati delle nostre operazioni ci risultano svariate vulnerabilità, molte anche particolarmente gravi, che comportano quindi seri rischi per i sistemi aziendali.

Alcune di esse permettono a potenziali malintenzionati di assumere il completo controllo dei sistemi aziendali, quindi avendo accesso a file e cartelle riservate, oppure il totale spegnimento ed eliminazione di qualsiasi servizio presente sul server analizzato.

Misure da adottare

Di seguito elencheremo una serie di misure da effettuare per risolvere i problemi di sicurezza presenti al interno dei sistemi aziendali da noi analizzati.

Partendo dalle vulnerabilità gravi:

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

In breve

C'è 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 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'internouna varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE)

Soluzione proposta

Aggiornare 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.

11356 (1) - NFS Exported Share Information Disclosure

In breve

E' possibile accedere da remoto alle cartelle NFS del server.

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione.

Un attaccante potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

Soluzione proposta

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

33850 (1) - Unix Operating System Unsupported Version Detection

In breve

Il sistema operativo non è più supportato.

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. Quindi è probabile che contenga vulnerabilità di sicurezza.

Soluzione proposta

Aggiornare il sistema a una versione di Unix supportata

136769 (1) - ISC BIND Service Downgrade / Reflected DoS

136808 (1) - ISC BIND Denial of Service

139915 (1) - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

In breve

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

Inoltre il server dei nomi remoto è interessato da una vulnerabilità di errore di asserzione.

Il server dei nomi remoto è affetto da una vulnerabilità Denial of Service.

Descrizione

secondo la sua versione auto-segnalata, 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.

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 di riflessione.

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.

In base al numero di versione auto-riportato, l'installazione di ISC BIND in esecuzione sul server dei nomi remoto 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. Pertanto, è affetto da una vulnerabilità di negazione del servizio (DoS) a causa di un errore di asserzione durante il tentativo di verificare una risposta troncata a una richiesta firmata da TSIG. Un utente malintenzionato remoto autenticato può sfruttare questo problema inviando una risposta troncata a una richiesta firmata TSIG per attivare un errore di asserzione, causando la chiusura del server.

Si noti che l'analisi non ha testato questo problema, ma si è invece basata solo sul numero di versione auto-riportato dell'applicazione.

Soluzione proposta

Aggiornare la versione di ISC BIND alla versione consigliata dal venditore.

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

Aggiorna a BIND 9.11.22, 9.16.6, 9.17.4 o successivo.

42256 (1) - NFS Shares World Readable

In breve

Il server remoto NFS esporta cartelle leggibili da tutti.

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 proposta

Impostare delle restrizioni adeguate alle cartelle NFS.

90509 (1) - Samba Badlock Vulnerability

In breve

Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

Descrizione

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 errata del livello di autenticazione sui canali RPC (Remote Procedure Call).

Un attaccante 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 la visualizzazione o la modifica di dati sensibili sulla sicurezza nel database di Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione proposta

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

52611 (1) - SMTP Service STARTTLS Plaintext Command Injection

In breve

Il servizio di posta remota consente l'inserimento di comandi in chiaro durante la negoziazione di un canale di comunicazione crittografato.

Descrizione

Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire a un utente malintenzionato remoto e non autenticato di inserire comandi durante la fase del protocollo di testo in chiaro che verranno eseguiti durante la fase del protocollo di testo cifrato.

Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o le credenziali SASL (Simple Authentication and Security Layer) associate.

Soluzione proposta

Contattare il fornitore per vedere se è disponibile un aggiornamento.

10407 (1) - X Server Detection

In breve

Un server X11 è in ascolto sull'host remoto.

Descrizione

L'host remoto esegue un server X11. X11 è un protocollo client-server che può essere utilizzato per visualizzare applicazioni grafiche in esecuzione su un determinato host su un client remoto.

Poiché il traffico X11 non è cifrato, è possibile che un utente malintenzionato intercetti la connessione.

Soluzione proposta

Limita l'accesso a questa porta. Se la funzionalità client/server X11 non viene utilizzata, disabilitare completamente il supporto TCP in X11 (-nolisten tcp).

Di seguito solo uno schema con quelle che sono considerate di livello info, cioè non una vera vulnerabilità, ma un modo di ottenere informazioni a riguardo del sistema:

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	-	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	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	10263	SMTP Server Detection
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	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	10342	VNC Software Detection
INFO	N/A	-	135860	WMI Not Available
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