192.168.50.101

8	4	16	6	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 104

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	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	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service

Nessus Essentials

Metasploit

‹ Back to My Scans

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | Vulnerabilities 62 | Remediations 2 | Notes 2 | History 1

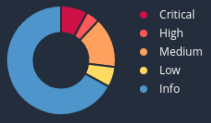
Filter | Search Vulnerabilities | 62 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:47 AM
End: Today at 9:24 AM
Elapsed: 37 minutes

Vulnerabilities



Il Ghostcat (CVE-2020-1938), noto anche come Apache Tomcat AJP Connector Request Injection, è una vulnerabilità critica scoperta nel protocollo AJP (Apache JServ Protocol) di Apache Tomcat, un server web e un server di servlet open-source. Questa vulnerabilità è stata identificata come un'opportunità per gli attaccanti di eseguire un attacco di traversal della directory e visualizzare file remoti sul server vulnerabile, inclusi file di configurazione sensibili.

Il problema principale riguarda la configurazione predefinita di Tomcat, che consente l'accesso non autorizzato al file di configurazione web.xml e ad altri file all'interno del contesto dell'applicazione web. Gli hacker possono sfruttare questa falla per leggere informazioni sensibili o eseguire altre azioni dannose sul server.

Il numero 51988 potrebbe essere associato a un ID di vulnerabilità specifico all'interno di un database o di un elenco di minacce noto come CVE (Common Vulnerabilities and Exposures). Tuttavia, non c'è un riferimento diretto a una vulnerabilità specifica con quel numero.

La "Bind Shell Backdoor" si riferisce a un tipo di backdoor inserito in un sistema che consente a un attaccante remoto di ottenere un accesso diretto e non autorizzato al sistema compromesso. Una "Bind Shell" si riferisce a una connessione aperta in ascolto su una porta specifica del sistema compromesso, consentendo all'attaccante di connettersi a essa da remoto e ottenere un accesso a livello di shell.

La rilevazione di una backdoor di tipo "Bind Shell" coinvolge spesso l'analisi delle porte aperte e delle connessioni di rete in entrata e in uscita per individuare attività sospette. I tool di rilevamento delle minacce e i meccanismi di sicurezza possono monitorare il traffico di rete e cercare segni di comunicazioni inusuali o di attività sospette che potrebbero indicare la presenza di un backdoor di questo tipo.

Il numero 20007 potrebbe essere associato a un'indicazione di vulnerabilità o a un codice di riferimento all'interno di strumenti di sicurezza, come i database di firme o di regole usati da software come intrusion detection system (IDS) o intrusion prevention system (IPS).

"SSL Version 2 and 3 Protocol Detection" fa riferimento alla capacità di rilevare e identificare l'uso dei protocolli SSL (Secure Sockets Layer) versione 2 e 3. Questi sono protocolli crittografici utilizzati per stabilire connessioni sicure su Internet, ma sono stati ormai considerati obsoleti e vulnerabili a diverse minacce di sicurezza, tra cui attacchi come POODLE (Padding Oracle On Downgraded Legacy Encryption).

A causa delle loro debolezze, le versioni SSL 2 e 3 sono state ampiamente disabilitate e rimosse in favore di versioni più sicure come TLS (Transport Layer Security). Tuttavia, i vecchi sistemi o le configurazioni non aggiornate potrebbero ancora utilizzare questi protocolli obsoleti, il che potrebbe essere considerato una potenziale vulnerabilità di sicurezza.

La rilevazione di queste versioni obsolete dei protocolli SSL è importante per identificare e mitigare possibili rischi per la sicurezza. I sistemi di rilevamento possono analizzare il traffico di rete e cercare segni dell'uso di SSL v2 e v3, fornendo all'amministratore di sistema o agli strumenti di sicurezza l'avviso necessario per effettuare le correzioni o le modifiche appropriate per mitigare questi rischi.