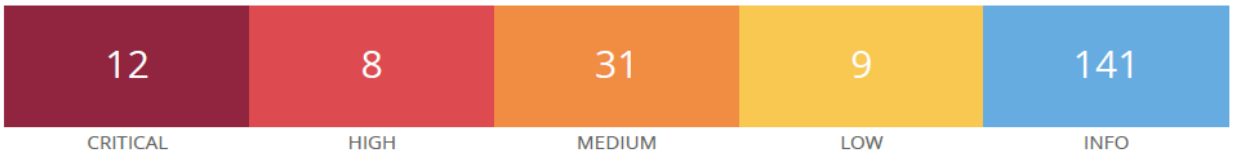
REPORT VULNERABILITA’



Informazioni Scan:

Inizio: Lunedì, 26 Febbraio 14:30:12 2024

Fine: Lunedì, 26 Febbraio 14:59:14 2024

Informazioni Host:

Nome Netbios: Metasploitable

IP: 192.168.1.101

MAC Address: 08:00:27:E5:4A:BF

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

CRITICAL

- **70728 - Apache PHP-CGI Remote Code Execution**

Sinossi: Il web server remoto contiene una versione di PHP che consente l'esecuzione di codice senza autorizzazione.

Descrizione: L'installazione di PHP sul web server remoto contiene un difetto che potrebbe consentire a un utente malintenzionato da remoto di passare argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Se ne potrebbe abusare per eseguire codice non autorizzato, rivelare il codice sorgente PHP, causare un arresto anomalo del sistema, ecc.

Soluzione: Aggiorna a PHP 5.3.13 / 5.4.3 o versioni successive

- **134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)**

Sinossi: Sull'host remoto è presente un connettore AJP vulnerabile.

Descrizione: È stata individuata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere file di applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile consenta il caricamento di file, un attaccante potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di vari tipi di file e ottenere l'esecuzione remota di codice (RCE).

Soluzione: Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o eseguire l'aggiornamento del server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.

- **51988 - Bind Shell Backdoor Detection**

Sinossi: L'host remoto potrebbe essere stato compromesso.

Descrizione: Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

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

- **20007 - SSL Version 2 and 3 Protocol Detection**

Sinossi: Il servizio remoto crittografa il traffico utilizzando un protocollo con debolezze conosciute.

Descrizione: Il servizio remoto accetta connessioni crittografate usando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diverse vulnerabilità crittografiche, tra cui:

- Uno schema di riempimento insicuro con cifrari CBC.
- Schemi di rinegoziazione e ripresa sessione insicuri.

Un attaccante può sfruttare queste vulnerabilità per condurre attacchi man-in-the-middle o per decifrare comunicazioni tra il servizio interessato e i client. Anche se SSL/TLS ha un modo sicuro per scegliere la versione più elevata supportata del protocollo (in modo che queste versioni siano utilizzate solo se il client o il server non supportano nulla di migliore), molti browser web lo implementano in modo insicuro, consentendo a un attaccante di declassare una connessione (come nel caso di POODLE). Pertanto, è consigliabile disabilitare completamente questi protocolli. Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. Alla data di applicazione indicata in PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di 'crittografia forte' del PCI SSC.

Soluzione: Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizzare invece TLS 1.2 (con suite di cifrari approvate) o versioni superiori.

- **125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)**

Sinossi: Il server web remoto ospita un'applicazione PHP colpita da una vulnerabilità di SQL injection (SQLi).

Descrizione: In base al numero di versione auto-dichiarato, l'applicazione phpMyAdmin ospitata sul server web remoto è precedente alla versione 4.8.6. Pertanto, è affetta da una vulnerabilità di SQL injection (SQLi) che si verifica nella funzione di progettazione di phpMyAdmin. Un attaccante remoto non autenticato può sfruttarla per iniettare o manipolare query SQL nel database di backend, risultando nella divulgazione o manipolazione di dati arbitrari. Si noti che Nessus non ha cercato di sfruttare questi problemi, ma si è invece basato solo sul numero di versione auto-dichiarato dall'applicazione.

Soluzione: Aggiornare a phpMyAdmin versione 4.8.6 o successiva. In alternativa, applicare le correzioni indicate negli avvisi del fornitore.

HIGH

- **90509 - Samba Badlock Vulnerability**

Sinossi: Un server SMB in esecuzione sull'host remoto è colpito dalla vulnerabilità Badlock.

Descrizione: La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è interessata da una falla, nota come Badlock, che si verifica nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione su canali Remote Procedure Call (RPC). Un attaccante uomo-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 degrado del livello di autenticazione, consentendo 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 Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione: Aggiornare a Samba versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.

- **19704 - TWiki 'rev' Parameter Arbitrary Command Execution**

Sinossi: Il server web remoto ospita un'applicazione CGI che è colpita da una vulnerabilità di esecuzione di comandi arbitrari.

Descrizione: La versione di TWiki in esecuzione sull'host remoto consente a un attaccante di manipolare l'input al parametro 'rev' al fine di eseguire comandi shell arbitrari sull'host remoto, subordinatamente ai privilegi dell'ID utente del server web.

Soluzione: Applicare il hotfix appropriato indicato nell'avviso del fornitore.

MEDIUM

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

Sinossi: Il server DNS remoto è affetto da una vulnerabilità di negazione del servizio.

Descrizione: In base al numero di versione auto-dichiarato, l'installazione di ISC BIND in esecuzione sul server DNS remoto è una 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 pertanto affetto da una vulnerabilità di negazione del servizio (DoS) a causa di un fallimento nell'asserzione durante il tentativo di verificare una risposta troncata a una richiesta firmata con TSIG. Un attaccante remoto autenticato può sfruttare questo problema inviando una risposta troncata a una richiesta firmata con TSIG per provocare un fallimento nell'asserzione, causando l'uscita del server. Si noti che Nessus non ha testato questo problema, ma si è invece basato solo sul numero di versione auto-dichiarato dall'applicazione.

Soluzione: Effettuare l'aggiornamento a BIND 9.11.22, 9.16.6, 9.17.4 o versioni successive.

LOW

- **70658 - SSH Server CBC Mode Ciphers Enabled**

Sinossi: Il server SSH è configurato per utilizzare il Cipher Block Chaining (CBC).

Descrizione: Il server SSH è configurato per supportare la crittografia Cipher Block Chaining (CBC). Ciò potrebbe consentire a un attaccante di recuperare il testo in chiaro dal testo cifrato. Si noti che questo plugin verifica solo le opzioni del server SSH e non controlla le versioni vulnerabili del software.

Soluzione: Contattare il fornitore o consultare la documentazione del prodotto per disabilitare la crittografia in modalità CBC e abilitare la crittografia in modalità CTR o GCM.