Università degli Studi di Salerno

Penetration Testing Report

SUNSET: SOLSTICE

Marika Spagna Zito | Corso di PTEH | A.A. 2023/2024

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

1. Executive Summary

Per il progetto del corso di Penetration Testing & Ethical Hacking dell'anno accademico 2023/2024, è stato eseguito un processo di penetration testing etico sulla macchina virtuale vulnerabile by design "Sunset: Solstice" disponibile sul sito VulnHub [1].

L'attività di penetration testing sulla macchina target ha avuto inizio il 24/06/2024. Per simulare un attacco svolto da un utente privo di informazioni, è stato condotto un testing di tipo black box: al tester non sono state fornite informazioni in merito all'asset.

L'obiettivo è stato quello di determinare l'esposizione dell'asset a possibili attacchi, valutandone il livello di sicurezza e identificandone le vulnerabilità. Il test ha simulato un piano d'attacco che un utente malevolo potrebbe utilizzare per compromettere la confidenzialità, l'integrità e la disponibilità della macchina.

Come risultato sono state individuate in totale 3 vulnerabilità di livello critico, 7 di livello alto, 13 di livello medio e 6 di livello basso. Questo indica che il livello di sicurezza della macchina in questione è estremamente basso e che non sono state implementate adeguate contromisure di sicurezza all'interno dell'ambiente.

Nelle sezioni successive tali vulnerabilità vengono dettagliate e corredate dalle opportune mitigazioni con l'obiettivo di mettere in sicurezza l'asset.

2. Engagement Highlights

L’attività di penetration testing è stata condotta per scopi accademici; quindi, non è stato necessario stabilire regole d'ingaggio tra le parti o firmare un accordo di non divulgazione. Ciò ha permesso un'analisi completa dell'asset, senza restrizioni sugli strumenti utilizzati.

3. Vulnerability Report

Durante l'analisi della macchina target sono state individuate alcune vulnerabilità che la espongono ad attacchi da parte di utenti malintenzionati. In particolare, le vulnerabilità individuate sono le seguenti:

- **Il sistema operativo ha raggiunto la fine del suo ciclo di vita** ciò vuol dire che il produttore ha interrotto il supporto ufficiale per questa versione. Utilizzare un sistema operativo in questa condizione può essere rischioso poiché non riceverà più aggiornamenti per la sicurezza e correzioni di bug.
- **Versione php non supportata:** La versione non supportata di PHP in esecuzione sul server web è vulnerabile a molte minacce, tra cui memory leak, attacchi DoS, out-of-bounds read, buffer overflow, falsificazione dei cookie e crittografia debole
- **L'intestazione anti-clickjacking X-Frame-Options non è presente.**
- **Il server FTP remoto consente accessi anonimi.** Questo potrebbe consentire a un utente malintenzionato di visualizzare, modificare o eliminare dati critici, a seconda delle autorizzazioni impostate per l'accesso anonimo.
- **File possono essere acceduti o eseguiti da remoto:** un utente malintenzionato potrebbe essere in grado di leggere file arbitrari sul server Web o eseguire comandi. Infatti, è stato possibile effettuare una RCE una Remote Code Execution.
- **Eseguibili con privilegi ingiustificati**: Sono stati identificati eseguibili con privilegi elevati che consentono a qualsiasi utente di eseguire codice arbitrario con autorizzazioni da amministratore.
- **Utilizzo di password di default e in chiaro**: Sono state scoperte password predefinite memorizzate in chiaro nei file di configurazione, prive di qualsiasi forma di cifratura. La conoscenza di queste credenziali permette a un potenziale attaccante di impersonare l'utente corrispondente.

4. Remediation Report

Per mitigare le vulnerabilità riscontrate durante l'attività di penetration testing bisognerebbe attuare le seguenti strategie di mitigazione:

- Passare a una versione più recente del sistema operativo supportata dal produttore. Questo può richiedere un aggiornamento diretto del sistema operativo esistente o una migrazione verso una nuova versione o piattaforma.
- Passare alla versione PHP più recente supportata, che include correzioni di sicurezza per le vulnerabilità menzionate.
- Configurare il server web per includere l'intestazione X-Frame-Options nelle risposte HTTP.
- Disabilitare l'accesso anonimo nelle impostazioni di configurazione del server FTP. Configura il server per richiedere l'autenticazione mediante nome utente e password per ogni connessione, applicando permessi appropriati per limitare l'accesso ai dati critici solo agli utenti autorizzati.
- Per prevenire l'accesso o l'esecuzione remota non autorizzata di file su un server Web ci sono diverse possibilità. Si potrebbe mantenere aggiornato il sistema operativo e il software del server con le patch di sicurezza più recenti. O configurare il server Web in modo sicuro, disabilitando le funzionalità non necessarie e utilizzando HTTPS per le comunicazioni sicure. Oppure implementare un firewall per limitare l'accesso al server e utilizzare un sistema robusto di autenticazione e autorizzazione per controllare l'accesso ai file e ai comandi.
- Abbassare i privilegi dei file eseguibili aventi privilegi ingiustamente elevati.
- Adottare password robuste per l'autenticazione degli utenti del sistema e implementare algoritmi di crittografia sicuri per proteggere le password nei file di configurazione.

5. Findings Summary

Durante un penetration testing, le vulnerabilità sono valutate in base al livello di rischio associato:

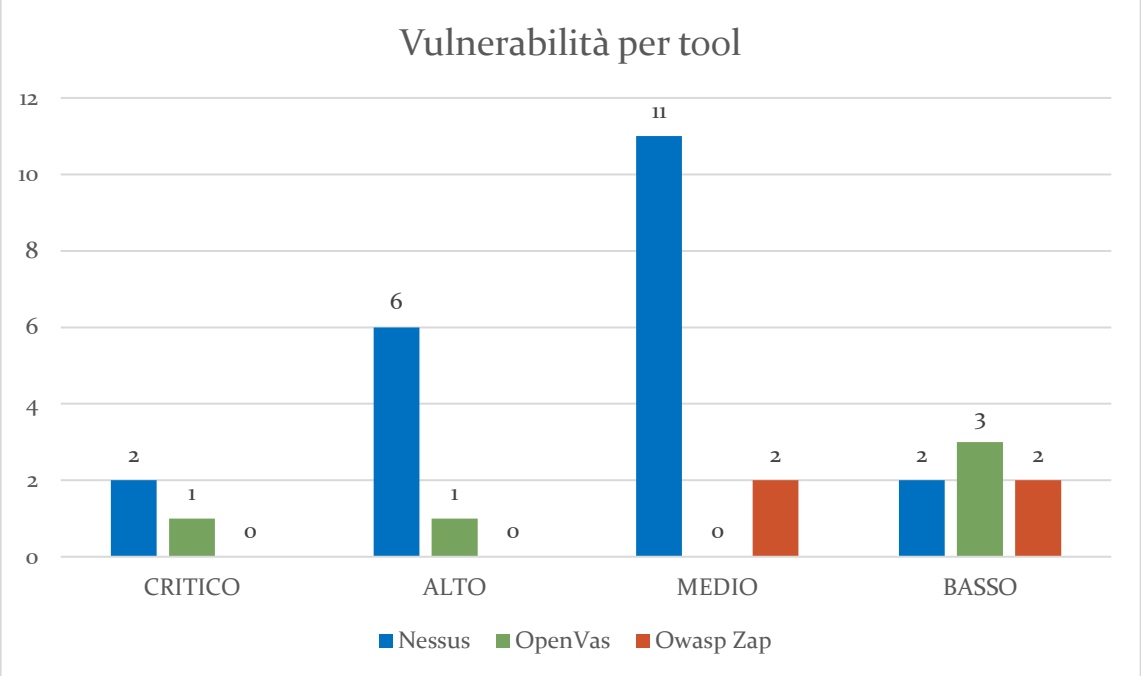
- **Critico:** vulnerabilità che rappresentano un grave pericolo per la sicurezza del sistema e che possono condurre a danni rilevanti al sistema;
- **Alto:** vulnerabilità di grande impatto che possono portare a importanti perdite di confidenzialità o integrità del sistema;
- **Medio:** vulnerabilità che richiedono particolari condizioni per essere sfruttate, ma che potrebbero compromettere il sistema;
- **Basso:** vulnerabilità non prioritarie e con un minimo impatto sul sistema;

Nel seguente report, come evidenziato nella prossima sezione, ogni livello di rischio è stato associato a un colore specifico: carminio per il rischio critico, rosso per il rischio alto, arancione per il rischio medio e giallo per il rischio basso.

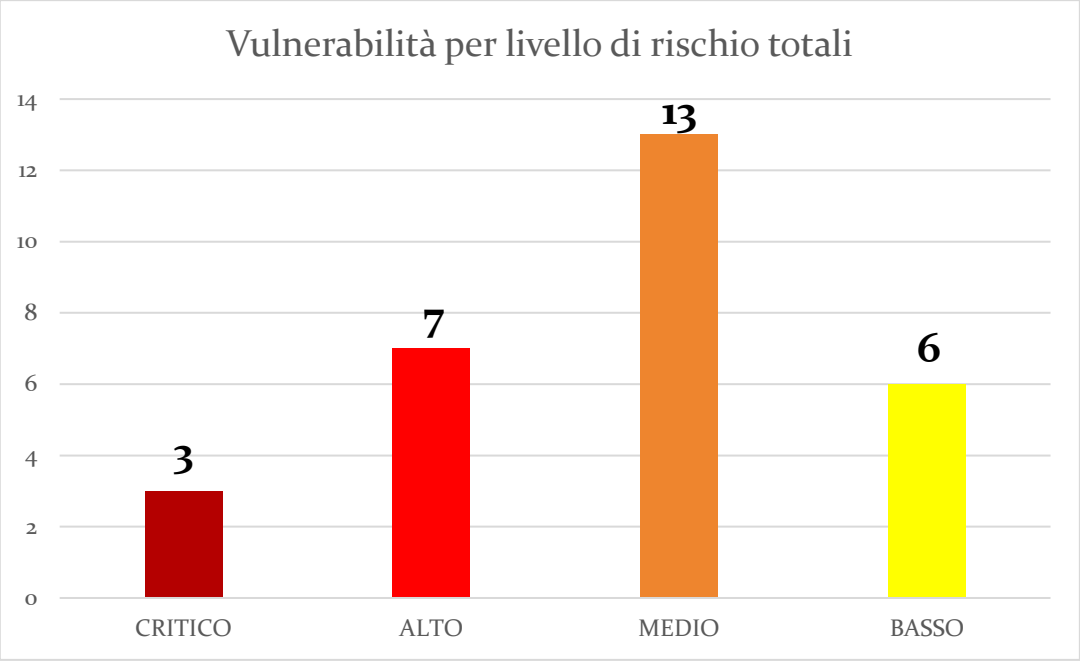
Queste vulnerabilità sono state individuate da tre tool:

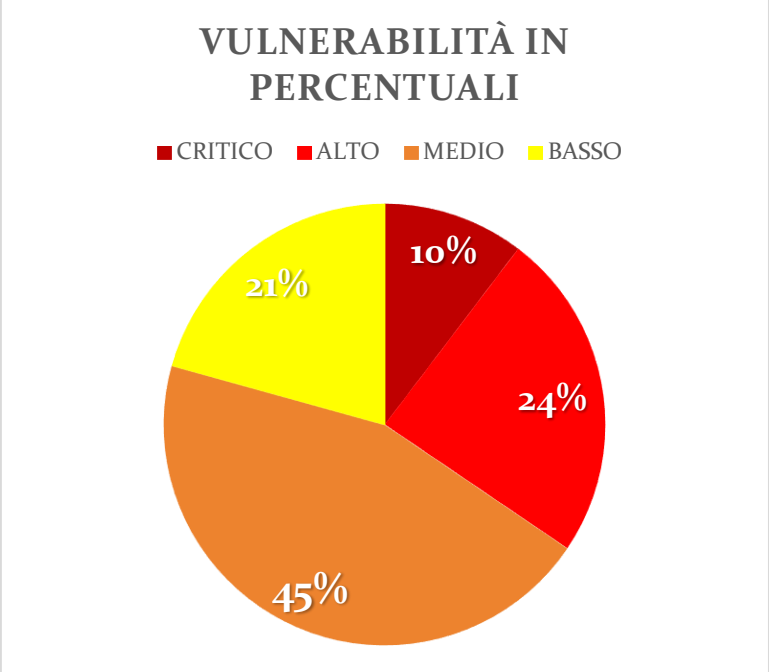
Nessus: 2 di livello critico, 6 di livello alto, 11 di livello medio, 1 di livello basso
OpenVas: 1 di livello critico, 1 livello alto, 2 di livello basso
Owasp Zap: 2 di livello medio e 2 di livello basso

Più un'altra vulnerabilità di livello basso individuata sia da Nessus e da OpenVas.



In totale otteniamo i seguenti dati:





6. Detailed Summary

In questa sezione verranno elencate e descritte in dettaglio tutte le vulnerabilità individuate manualmente e tramite i tool automatici

6.1 Vulnerabilità classificate: CRITICAL

Operating System (OS) End Of Life (EOL) Detection
Sinossi:
Rilevamento fine ciclo di vita del sistema operativo
Descrizione:
Il sistema operativo sull'host remoto ha raggiunto la fine del suo ciclo di vita e non deve più essere utilizzato.
Soluzione:
Aggiornare il sistema operativo sull'host remoto a una versione ancora supportata e che riceve aggiornamenti di sicurezza dal fornitore
Rischio:
Critico
CVSS v3.0 Base Score:
10
Riferimenti:
https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.103674

PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da molteplici vulnerabilità.
Descrizione:
Secondo il banner, la versione di PHP in esecuzione sul server web remoto è una tra le seguenti: o è una versione compresa tra 7.2.x e 7.2.28, o compresa tra 7.3.x e 7.3.15, oppure tra 7.4.x e 7.4.3. Pertanto, è affetta da molteplici vulnerabilità: - Una condizione di overflow del buffer basato su heap esiste nella funzione phar_extract_file() a causa della terminazione errata del ciclo. Un attaccante remoto non autenticato può sfruttare questa vulnerabilità per causare una condizione di denial of service o per eseguire codice arbitrario. (CVE-2020-7061) - Una vulnerabilità di denial of service (DoS) esiste nelle funzioni PHP SessionUpload Progress a causa della dereferenziazione di un puntatore nullo. Un attaccante remoto non autenticato può sfruttare questo problema per causare l'interruzione del servizio php. (CVE-2020-7062) - Un problema di permessi di file non sicuri nella funzione buildFromIterator assegna tutti i permessi di accesso ai file Tar. (CVE-2020-7063)
Soluzione:
Aggiornare alla versione PHP 7.2.28, 7.3.15, 7.4.3 o successiva.
CVE:
CVE-2020-7061, CVE-2020-7062, CVE-2020-7063
Rischio:
Critico
CVSS v3.0 Base Score:
9.1
Riferimenti:
https://www.tenable.com/plugins/nessus/134162 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7061 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7062 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7063

PHP Unsupported Version Detection
Sinossi:
L'host remoto contiene una versione non supportata di un linguaggio di scripting per applicazioni web
Descrizione:
Secondo la sua versione, l'installazione di PHP sull'host remoto non è più supportata. La mancanza di supporto implica che non verranno rilasciate nuove patch di sicurezza per il prodotto da parte del fornitore. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.
Soluzione:
Eseguire l'upgrade a una versione di PHP attualmente supportata.
Rischio:
Critico
CVSS v3.0 Base Score:
10
Riferimenti:
https://www.tenable.com/plugins/nessus/58987

6.2 Vulnerabilità classificate: HIGH

PHP 7.3.x < 7.3.16 Multiple Vulnerabilities
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da molteplici vulnerabilità.
Descrizione:
La versione di PHP in esecuzione sul server web remoto è compresa tra 7.3.x e 7.3.16. Pertanto, è affetta dalle seguenti vulnerabilità: - Una lettura fuori dai limiti che risulta nell'uso di un valore non inizializzato in exif. (CVE-2020-7064) - Un overflow del buffer dello stack in mb_strtolower() permette la sovrascrittura di un buffer allocato nello stack con un array in overflow proveniente da .rodata. (CVE-2020-7065) - La funzione get_headers() tronca silenziosamente tutto ciò che segue un byte nullo nell'URL che utilizza. Un attaccante remoto non autenticato può sfruttare questa vulnerabilità per divulgare informazioni sensibili o causare l'elaborazione imprevista di dati controllati dall'attaccante da parte del server web. (CVE-2020-7066)
Soluzione:
Aggiornare alla versione PHP 7.3.16 o successiva.
CVE:
CVE-2020-7064, CVE-2020-7065, CVE-2020-7066
Rischio:
Alto
CVSS v3.0 Base Score:
8.8
Riferimenti:
https://www.tenable.com/plugins/nessus/134944 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7064 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7065 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7066

Squid Multiple 0-Day Vulnerabilities (Oct 2023)
Sinossi:
Squid è soggetto a molteplici vulnerabilità zero-day (0-day).
Descrizione:
Ci sono diversi problemi critici non ancora risolti al fornitore. Tra questi ci sono vulnerabilità come buffer overflow e use-after-free nelle richieste TRACE e nell'autenticazione Digest, insieme a perdite di memoria nell'analisi delle risposte HTTP e nei processi di gestione degli errori ESI.
Soluzione:
Non è disponibile alcuna soluzione nota.
Rischio:
Alto
CVSS v3.0 Base Score:
7.8
Riferimenti:
https://www.mageni.net/vulnerability/squid-multiple-0-day-vulnerabilities-oct-2023-100439

PHP < 7.3.24 Multiple Vulnerabilities
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da molteplici vulnerabilità.
Descrizione:
La versione di PHP in esecuzione sul server Web remoto è precedente alla 7.3.24 la quale è affetta da molteplici vulnerabilità.
Soluzione:
Aggiornare alla versione PHP 7.3.24 o successiva.
Rischio:
Alto
CVSS v3.0 Base Score:
7.5

Riferimenti:
https://www.tenable.com/plugins/nessus/142591

PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da una vulnerabilità di tipo memory leak.
Descrizione:
La versione di PHP installata sull'host remoto è una versione del tipo 7.2.x o 7.2.3 ed è precedente a 7.3.22. Questa versione è vulnerabile a una perdita di memoria nel componente LDAP. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per causare una condizione di denial-of-service
Soluzione:
Aggiornare alla versione PHP 7.3.22 o successiva.
Rischio:
Alto
CVSS v3.0 Base Score:
7.5
Riferimenti:
https://www.tenable.com/plugins/nessus/140532

PHP 7.3.x < 7.3.27 / 7.4.x < 7.4.15 / 8.x < 8.0.2 DoS
Sinossi:
La versione di PHP in esecuzione sul server web remoto è soggetta a una vulnerabilità di tipo denial of service (DoS).
Descrizione:
La versione di PHP installata sull'host remoto è compresa tra 7.3.x e 7.3.27, compresa tra 7.4.x e 7.4.15, oppure compresa tra 8.x e 8.0.2. Di conseguenza, è vulnerabile a una vulnerabilità di tipo denial of service (DoS) dovuta a un dereferenziamento nullo in SoapClient. Un attaccante remoto non autenticato può sfruttare questa vulnerabilità

fornendo un XML alla funzione query() di SoapClient senza un campo esistente, il che può causare il crash di PHP.
Soluzione:
Aggiornare alla versione PHP 7.3.27, 7.4.15, 8.0.2 o successive.
CVE:
CVE-2021-21702
Rischio:
Alto
CVSS v3.0 Base Score:
7.5
Riferimenti:
https://www.tenable.com/plugins/nessus/146311 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21702

PHP 7.3.x < 7.3.17 Out of Bounds Read Vulnerability
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da molteplici vulnerabilità.
Descrizione:
La versione di PHP in esecuzione sul server web remoto è compresa tra 7.3.x e 7.3.17. È, quindi, affetto da un errore del tipo out-of-bounds read nel suo componente di decodifica URL dovuto a una insufficiente convalida dell'input fornito dall'utente. Un aggressore remoto non autenticato può sfruttare questo, inviando richieste appositamente predisposte, per causare una condizione di negazione del servizio (DoS) o l'esecuzione di codice arbitrario.
Soluzione:
Aggiornare alla versione PHP 7.3.17 o successiva.
CVE:
CVE-2020-7067

Rischio:
Alto
CVSS v3.0 Base Score:
7.5
Riferimenti:
https://www.tenable.com/plugins/nessus/135918 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7067

PHP 7.3.x < 7.3.32
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da molteplici vulnerabilità.
Descrizione:
Nelle versioni di PHP 7.3.x fino e inclusa la 7.3.31, 7.4.x inferiore alla 7.4.25 e 8.0.x inferiore alla 8.0.12, quando si esegue PHP FPM SAPI con il processo principale del demone FPM in esecuzione come root e i processi figlio lavoratori in esecuzione come utenti a privilegi inferiori, è possibile che i processi figlio accedano alla memoria condivisa con il processo principale e vi scrivano, modificandola in modo tale che il processo radice effettui letture e scritture di memoria non valide, il che potrebbe essere utilizzato per effettuare privilege escalation da un utente non privilegiato locale all'utente root.
Soluzione:
Aggiornare alla versione PHP 7.3.32 o successiva.
CVE:
CVE-2021-21703
Rischio:
Alto
CVSS v3.0 Base Score:
7.0
Riferimenti:
https://www.tenable.com/plugins/nessus/154663 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21703

6.3 Vulnerabilità classificate: MEDIUM

PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x < 7.4.11 Multiple Vulnerabilities
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da molteplici vulnerabilità.
Descrizione:
La versione di PHP in esecuzione sul server web remoto è compresa tra 7.2.x e 7.2.34, 7.3.x precedente alla 7.3.23 o 7.4.x precedente alla 7.4.11. Di conseguenza, è affetta da diverse vulnerabilità: - Esiste una vulnerabilità di crittografia debole nella funzione openssl_encrypt di PHP a causa della mancata utilizzazione di tutti i byte IV forniti. Un attaccante remoto non autenticato potrebbe sfruttare questo problema per ridurre il livello di sicurezza fornito dallo schema di crittografia o compromettere l'integrità dei dati crittografati (CVE-2020-7069). - Esiste una vulnerabilità di falsificazione dei cookie nella funzionalità di elaborazione HTTP di PHP. Un attaccante remoto non autenticato potrebbe sfruttare questo problema per falsificare i cookie HTTP che dovevano essere sicuri (CVE-2020-7070).
Soluzione:
Aggiornare alla versione PHP 7.2.34, 7.3.23, 7.4.11 o successive.
CVE:
CVE-2020-7069, CVE-2020-7070
Rischio:
Medio
CVSS v3.0 Base Score:
6.5
Riferimenti:
https://www.tenable.com/plugins/nessus/141355 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7069 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7070

Exim <= 4.96.2 libspf2 RCE Vulnerability (Sep 2023)
Sinossi:
Exim è soggetto a una vulnerabilità di esecuzione di codice remoto (RCE) in libspf2
Descrizione:
Il difetto specifico esiste nell'analisi delle macro SPF. Quando si analizzano le macro SPF, il processo non convalida correttamente i dati forniti dall'utente, il che può causare un underflow di interi prima della scrittura in memoria. Un aggressore può sfruttare questa vulnerabilità per eseguire codice nel contesto dell'account di servizio.
Soluzione:
Non è disponibile alcuna soluzione nota.
CVE:
CVE-2023-42118
Rischio:
Medio
CVSS v3.0 Base Score:
6.8
Riferimenti:
https://pentest-tools.com/vulnerabilities-exploits/exim-4962-libspf2-rce-vulnerability-sep-2023_19281 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42118

Missing Anti-clickjacking Header
Sinossi:
L'intestazione anti-clickjacking X-Frame-Options non è presente.
Descrizione:
La risposta del server non include né l'header Content-Security-Policy con la direttiva 'frame-ancestors' né l'header X-Frame-Options per proteggere contro gli attacchi di 'ClickJacking'.
Soluzione:

I browser Web moderni supportano le intestazioni HTTP Content-Security-Policy e X-Frame-Options. Assicurarsi che uno di essi sia impostato su tutte le pagine Web restituite dal sito/app.
CVE:
CVE-2018-17192
Rischio:
Medio
CVSS v3.0 Base Score:
6.5
Riferimenti:
https://www.zaproxy.org/docs/alerts/10020-1/ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17192

Anonymous FTP Login Reporting
Sinossi:
Il server FTP remoto consente accessi anonimi.
Descrizione:
L'accesso FTP anonimo rappresenta una vulnerabilità significativa dal momento che permette agli utenti di connettersi al server FTP senza necessità di autenticazione diretta tramite un account specifico. Utilizzando comunemente "anonimo" o "ftp" come nome utente e un indirizzo e-mail come password, che spesso non viene verificata, gli utenti possono accedere a file sensibili sul server. Questo potrebbe consentire a un utente malintenzionato di visualizzare, modificare o eliminare dati critici, a seconda delle autorizzazioni impostate per l'accesso anonimo.
Soluzione:
Disabilitare gli accessi anonimi. Verificare e impostare correttamente i permessi di accesso ai file e alle directory sul server FTP. Limitare l'accesso solo ai file e alle directory necessarie per ogni utente autorizzato.
CVE:
CVE-1999-0497
Rischio:
Medio

CVSS v3.0 Base Score:
6.4
Riferimenti:
https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.900600 https://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0497

Content Security Policy (CSP) Header Not Set
Sinossi:
Il Content Security Policy non è impostato.
Descrizione:
Content Security Policy (CSP) è un ulteriore livello di sicurezza che aiuta a rilevare e mitigare determinati tipi di attacchi, tra cui Cross Site Scripting (XSS) e attacchi di iniezione di dati. Questi attacchi vengono utilizzati per tutto, dal furto di dati alla deturpazione del sito o alla distribuzione di malware. CSP fornisce un set di intestazioni HTTP standard che consentono ai proprietari di siti Web di dichiarare fonti approvate di contenuti che i browser dovrebbero essere autorizzati a caricare su quella pagina: i tipi coperti sono JavaScript, CSS, frame HTML, font, immagini e oggetti incorporabili come applet Java, ActiveX, file audio e video.
Soluzione:
Assicurarsi che il server web, server delle applicazioni, sistema di bilanciamento del carico, ecc. sia configurato per impostare l'intestazione Content-Security-Policy.
CVE:
CVE-2018-5164
Rischio:
Medio
CVSS v3.0 Base Score:
6.1
Riferimenti:
https://www.zaproxy.org/docs/alerts/10038-1/ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5164

SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
Sinossi:
Il server SSH remoto è vulnerabile a un attacco di troncamento del prefisso MITM (Man-in-the-Middle)
Descrizione:
Il server SSH remoto è vulnerabile a una debolezza di troncamento del prefisso MITM (Man-in-the-Middle) nota come Terrapin. Questo può permettere a un attaccante remoto in mezzo alla comunicazione di eludere i controlli di integrità e abbassare la sicurezza della connessione.
Soluzione:
Contatta il fornitore per un aggiornamento che includa contromisure rigorose per lo scambio delle chiavi oppure disabilita gli algoritmi interessati.
CVE:
CVE-2023-48795
Rischio:
Medio
CVSS v3.0 Base Score:
5.9
Riferimenti:
https://www.tenable.com/plugins/nessus/187315 https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-48795

CGI Generic Path Traversal
Sinossi:
È possibile accedere o eseguire file arbitrari sull'host remoto.
Descrizione:
Il server web remoto ospita script CGI che non sanificano adeguatamente le stringhe di richiesta e sono vulnerabili a directory traversal o inclusione di file locali. Sfruttando questo problema, un attaccante potrebbe essere in grado di leggere file arbitrari sul server web o eseguire comandi.
Soluzione:

Limitare l'accesso all'applicazione vulnerabile. Contattare il venditore per ottenere una patch o eseguire un aggiornamento per risolvere le vulnerabilità di path traversal.
Rischio:
Medio
CVSS v3.0 Base Score:
5.3
Riferimenti:
https://www.tenable.com/plugins/nessus/39467

PHP 7.3.x < 7.3.26 / 7.4.x < 7.4.14 / 8.x < 8.0.1 Input Validation Error
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da un errore di validazione dell'input.
Descrizione:
La versione di PHP installata sull'host remoto è compresa tra 7.3.x e 7.3.26, tra 7.4.x e 7.4.14, o infine tra 8.x e 8.0.1. Di conseguenza, è affetta da un errore di validazione dell'input a causa di una validazione insufficiente di un URL, come specificato nei log delle modifiche delle rispettive versioni corrette. Un attaccante remoto non autenticato può sfruttare questo problema includendo un carattere '@' per aggirare il filtro dell'URL.
Soluzione:
Aggiornare alla versione PHP 7.3.26, 7.4.14, 8.0.1 o successive.
CVE:
CVE-2023-48795
Rischio:
Medio
CVSS v3.0 Base Score:
5.9
Riferimenti:
https://www.tenable.com/plugins/nessus/187315 https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-48795

PHP 7.3.x < 7.3.33
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da molteplici vulnerabilità.
Descrizione:
Nelle versioni di PHP comprese tra 7.3.x e 7.3.33, alcune funzioni di analisi XML, come simplexml_load_file(), decodificano l'URL del nome del file passato. Se tale nome del file contiene un carattere NULL codificato nell'URL, questo potrebbe causare l'interpretazione da parte della funzione come fine del nome file, interpretandolo quindi diversamente da quanto inteso dall'utente, il che potrebbe portare alla lettura di un file diverso da quello previsto. (CVE-2021-21707).
Soluzione:
Aggiornare alla versione PHP 7.3.33 o successiva.
CVE:
CVE-2021-21707
Rischio:
Medio
CVSS v3.0 Base Score:
5.3
Riferimenti:
https://www.tenable.com/plugins/nessus/155590 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21707

PHP < 7.3.28 Email Header Injection
Sinossi:
La versione di PHP in esecuzione sul server web remoto è affetta da una vulnerabilità del tipo email header injection.
Descrizione:

La versione di PHP in esecuzione sul server web remoto è precedente alla 7.3.28. Pertanto, è affetta da una vulnerabilità di injection nelle intestazioni delle email, dovuta a un mancato trattamento corretto delle sequenze CR-LF nei campi delle intestazioni. Un attaccante remoto non autenticato può sfruttare questo problema inserendo caratteri di salto riga nelle intestazioni delle email per ottenere il pieno controllo del contenuto delle intestazioni delle email.
Soluzione:
Aggiornare alla versione PHP 7.3.28 o successiva.
Rischio:
Medio
CVSS v3.0 Base Score:
5.3
Riferimenti:
https://www.tenable.com/plugins/nessus/152853

SMB Signing not required
Sinossi:
La firma non è richiesta sul server SMB remoto.
Descrizione:
La firma non è richiesta sul server SMB remoto. Un attaccante remoto non autenticato può sfruttare questa vulnerabilità per condurre attacchi man-in-the-middle contro il server SMB.
Soluzione:
Imposta l'obbligo di firma dei messaggi nella configurazione dell'host. Su Windows, questa impostazione si trova nella politica denominata 'Microsoft network server: Digitally sign communications (always)'. Su Samba, l'impostazione si chiama 'server signing'. Consulta i link correlati per ulteriori dettagli.
Rischio:
Medio
CVSS v3.0 Base Score:
5.3
Riferimenti:

https://www.tenable.com/plugins/nessus/57608

Web Application Information Disclosure
Sinossi:
L'applicazione web remota divulga informazioni sul percorso (path).
Descrizione:
Almeno una delle applicazioni web ospitate sul server web remoto divulga il percorso fisico delle sue directory quando viene inviata una richiesta malformata. La divulgazione di questo tipo di informazioni può aiutare un attaccante a perfezionare gli attacchi contro l'applicazione e il suo backend.
Soluzione:
Filtra i messaggi di errore che contengono informazioni sul percorso (path).
Rischio:
Medio
CVSS v3.0 Base Score:
5.0
Riferimenti:
https://www.tenable.com/plugins/nessus/57640

FTP Unencrypted Cleartext Login
Sinossi:
L'host remoto esegue un servizio FTP che consente l'accesso in chiaro tramite connessioni non crittografate.
Descrizione:
L'host remoto esegue un servizio FTP che consente accessi in chiaro tramite connessioni non crittografate. Un aggressore può scoprire nomi di accesso e password intercettando il traffico verso il servizio FTP.
Soluzione:
Abilitare FTPS o richiedere la connessione tramite il comando 'AUTH TLS'.
Rischio:

Medio
CVSS v3.0 Base Score:
4.8
Riferimenti:
https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108528

6.4 Vulnerabilità classificate: LOW

Server Leaks Version Information via "Server" HTTP Response Header Field
Sinossi:
Il server rilascia informazioni sulla versione tramite il campo di intestazione HTTP "Server".
Descrizione:
Il server web/applicativo sta rilasciando informazioni sulla versione tramite l'intestazione HTTP "Server" nella risposta. L'accesso a tali informazioni potrebbe facilitare agli aggressori l'identificazione di altre vulnerabilità a cui è soggetto il tuo server web/applicativo.
Soluzione:
Assicurarsi che il tuo server web, il server applicativo, il bilanciatore del carico, ecc. siano configurati per sopprimere l'intestazione "Server" o fornire dettagli generici.
Rischio:
Basso
CVSS v3.0 Base Score:
3.1
Riferimenti:
https://www.zaproxy.org/docs/alerts/10036-2/

X-Content-Type-Options Header Missing
Sinossi:
L'intestazione X-Content-Type-Options è mancante.
Descrizione:
L'intestazione Anti-MIME-Sniffing X-Content-Type-Options non è stata impostata su 'nosniff '. Ciò consente alle vecchie versioni di Internet Explorer e Chrome di eseguire lo sniffing MIME sul corpo della risposta, causando potenzialmente l'interpretazione e la visualizzazione del corpo della risposta come un tipo di contenuto diverso dal tipo di contenuto dichiarato. Le versioni correnti e legacy di Firefox utilizzeranno il tipo di contenuto dichiarato (se ne è impostato uno), anziché eseguire lo sniffing MIME.
Soluzione:
Assicurarsi che l'applicazione/server web imposti l'intestazione Content-Type in modo appropriato e che imposti l'intestazione X-Content-Type-Options su 'nosniff'

per tutte le pagine web. Se possibile, assicurarsi che l'utente finale utilizzi un browser web moderno e conforme agli standard che non esegua affatto lo sniffing MIME o che possa essere indirizzato dall'applicazione web/server web a non eseguire lo sniffing MIME.
Rischio:
Basso
CVSS v3.0 Base Score:
3.1
Riferimenti:
https://www.zaproxy.org/docs/alerts/10021/

PHP 7.3.x < 7.3.21 Use-After-Free Vulnerability
Sinossi:
La versione di PHP in esecuzione sul server Web remoto è affetta da una vulnerabilità use-after-free.
Descrizione:
La versione di PHP in esecuzione sul server web remoto è compresa tra 7.3.x e 7.3.21. È quindi interessata da una vulnerabilità use-after-free nella funzione phar_parse dovuta alla cattiva gestione della variabile actual_alias. Un aggressore remoto non autenticato potrebbe sfruttare questo problema dereferenziando un puntatore liberato, il che potrebbe portare all'esecuzione di codice arbitrario.
Soluzione:
Aggiornare alla versione PHP 7.3.21
CVE:
CVE-2020-7068
Rischio:
Basso
CVSS v3.0 Base Score:
3.6
Riferimenti:

https://www.tenable.com/plugins/nessus/139569 https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-7068

Weak MAC Algorithm(s) Supported (SSH)
Sinossi:
Sono supportati algoritmi MAC deboli (SSH).
Descrizione:
Il server SSH remoto è configurato per consentire o supportare algoritmi MAC deboli.
Soluzione:
Disabilitare gli algoritmi MAC deboli segnalati.
Rischio:
Basso
CVSS v3.0 Base Score:
2.6
Riferimenti:
https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.105610

TCP Timestamps Information Disclosure vulnerability
Sinossi:
Vulnerabilità di divulgazione delle informazioni sui timestamp TCP.
Descrizione:
Vulnerabilità di divulgazione delle informazioni sui timestamp TCP rilevata in una scansione di sicurezza sull'indirizzo IP del server virtuale. Le informazioni sui tempi di attività, se combinate con altre tecniche di rilevamento delle impronte digitali del sistema, possono identificare sufficientemente un sistema per un utente malintenzionato come un obiettivo potenzialmente utile per un attacco.
Soluzione:
Disattivare l' opzione Timestamp Extension for High Performance (RFC 1323) nel profilo TCP utilizzato per il server virtuale interessato.
Rischio:
Basso

CVSS v3.0 Base Score:
2.1
Riferimenti:
https://my.f5.com/manage/s/article/K000137636

ICMP Timestamp Request Remote Date Disclosure
Sinossi:
È possibile determinare l'ora esatta impostata sull'host remoto.
Descrizione:
L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un utente malintenzionato di conoscere la data impostata sulla macchina presa di mira, il che può aiutare un utente malintenzionato remoto non autenticato a sconfiggere i protocolli di autenticazione basati sul tempo. I timestamp restituiti dalle macchine che eseguono Windows Vista/7/2008/2008 R2 sono deliberatamente errati, ma in genere entro 1000 secondi dall'ora effettiva del sistema.
Soluzione:
Filtrare le richieste di timestamp ICMP (13) e le risposte di timestamp ICMP in uscita.
CVE:
CVE-1999-0524
Rischio:
Basso
CVSS v3.0 Base Score:
2.1
Riferimenti:
https://www.tenable.com/plugins/nessus/10114 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0524

References

[1] https://www.vulnhub.com/entry/sunset-solstice,499/

[2] https://www.cvedetails.com/

[3] https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-613554/Apache-Http-Server-2.4.38.html?page=1&order=3&trc=50&sha=bc7ece1671d203fba35b319b70e528299a938cee

[4] https://www.cybersecurity-help.cz/

[5] https://www.tenable.com/

[6] https://www.cybersecurity-help.cz/vdb/php_group/php/7.3.14/

[7] https://www.tenable.com/plugins/was/98992