Università degli Studi di Salerno

Penetration Testing Report

HARRY POTTER: NAGINI

Professore
Arcangelo Castiglione

Studente
Giuseppe Cardaropoli
Matricola: 0522501310

Corso di Penetration Testing & Ethical Hacking
A.A. 2022/2023

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

1. Executive Summary

Come attività progettuale è stato condotto un processo di penetration testing etico della macchina virtuale **HarryPotter: Nagini**, presente sulla piattaforma open-source Vulnhub e reperibile al seguente indirizzo: https://www.vulnhub.com/entry/harrypotter-nagini,689/

È stato utilizzato un approccio **Black Box**, ovvero il processo è stato svolto senza alcuna conoscenza preventiva relativa alla macchina target. Inoltre, come metodologia di riferimento è stato utilizzato il **Framework Generale per il Penetration Testing** (**FGPT**).

Tutte le attività sono state svolte in modo da simulare le possibili azioni di un attaccante malizioso. Il processo di penetration testing è stato svolto con i seguenti obiettivi:

- Stabilire il livello di sicurezza dell'asset;
- Determinare se un attaccante remoto può penetrare le difese dell'asset;
- Stimare l'impatto di una eventuale intrusione.

Durante il test si è cercato di identificare e sfruttare le vulnerabilità che potrebbero permettere ad un attaccante di ottenere accesso non autorizzato ai dati e/o di eseguire codice sulla macchina target.

Come risultato sono state trovate 7 vulnerabilità di livello critico, 4 di livello alto e 11 di livello medio. Questo indica che il livello di sicurezza della macchina in questione è estremamente basso e che non sono state messe in atto contromisure appropriate.

Questo report contiene un'analisi delle vulnerabilità riscontrare insieme ad una serie di raccomandazioni e contromisure per correggerle.

2. Vulnerability Report

Durante l'analisi della macchina target sono state individuate alcune vulnerabilità che la espongono ad attacchi da parte di utenti malintenzionati.

Sono state trovare password poco sicure e conservate in chiaro all'interno di semplici file di testo senza nessun meccanismo di cifratura. La conoscenza di tali credenziali consente ad un attaccante di impersonificare il relativo utente.

Sono stati trovati file di configurazione leggibili da qualunque utente tramite una semplice richiesta HTTP. All'interno di questi file è stato possibile individuare la tipologia di database installato sulla macchina ed il nome dell'utente che ha accesso al database. Inoltre, sempre all'interno del file di configurazione, è possibile notare come tale utente è sprovvisto di password.

Quest'ultima vulnerabilità consente ad un'utente malintenzionato di eseguire codice remoto, in particolar modo query SQL. Questo significa che un attaccante può leggere, modificare e/o cancellare le tabelle del database. Infatti, è stato possibile modificare la password dell'amministratore di Joomla in modo tale da impersonificarlo.

Inoltre, sono stati trovati eseguibili con privilegi ingiustamente elevati. Uno di questi consente la copia di file. Questo eseguibile è stato utilizzato per la copia di una chiave SSH, generata dall'attaccante, all'interno del file contenente le chiavi autorizzate di un certo utente. In questo modo l'attaccante può ottenere un accesso da remoto tramite SSH come utente privilegiato.

Infine, è stato riscontrato che sulla macchina è installato un sistema operativo e degli applicativi con versioni obsolete che presentano molteplici vulnerabilità.

3. Remediation Report

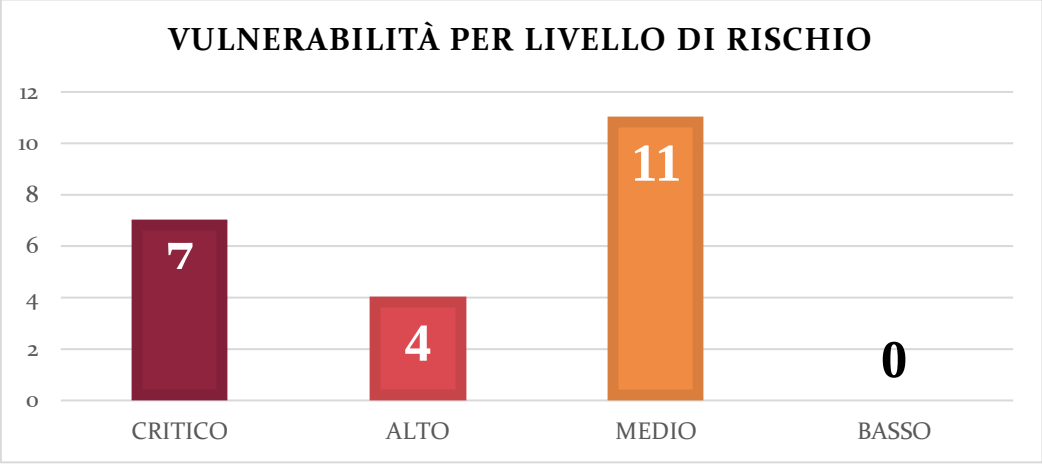
Per mitigare le vulnerabilità riscontrate durante l'attività di penetration testing bisognerebbe attuare le seguenti strategie di mitigazione:

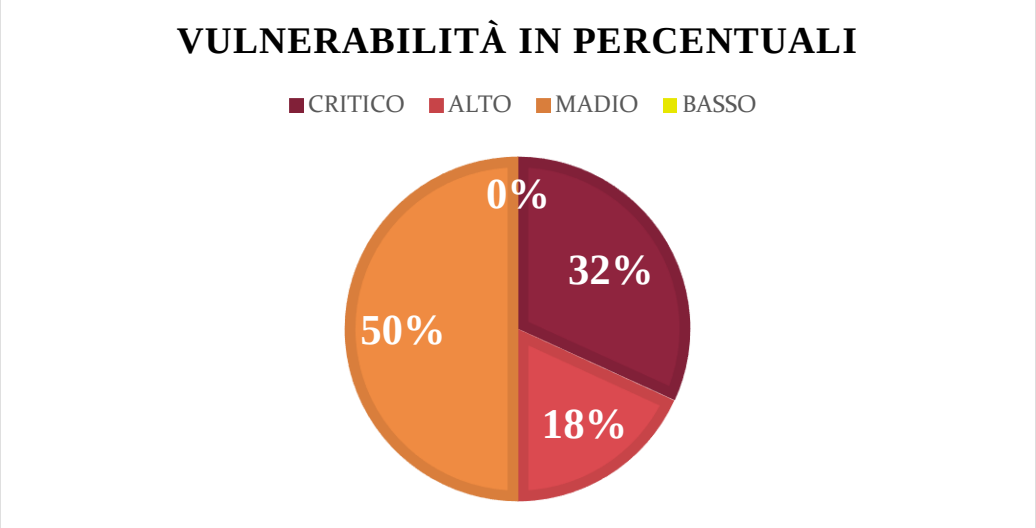
- Utilizzare password più sicure per l'autenticazione degli utenti del sistema. Questo è particolarmente importante dato che la macchina consente l'accesso da remoto tramite SSH;
- Impedire l'accesso non autorizzato a file contenenti informazioni sensibili;
- Assegnare una password sicura all'utente che ha accesso al database. Questo aspetto è cruciale perché tale utente è sprovvisto di password e ciò consente ad un attaccante l'esecuzione di query SQL attraverso le quali può leggere, modificare e/o cancellare le tabelle del database;
- Abbassare i privilegi dei file eseguibili aventi privilegi ingiustamente elevati;
- Aggiornare il sistema operativo e gli applicativi installati sulla macchina a delle versioni più recenti.

4. Finding Summary

Durante il processo di penetration testing sono state trovate una serie di vulnerabilità. A ciascuna di esse è associato un livello di rischio:

- **Critico**: le vulnerabilità di questo tipo dovrebbero essere sistemate immediatamente in quanto rappresentano un serio pericolo per la sicurezza del sistema. Il loro sfruttamento non richiede tecniche avanzate e/o una particolare conoscenza della macchina target;
- **Alto**: queste vulnerabilità andrebbero sistemate al più presto in quanto mettono il sistema in pericolo. Sono in genere un po' più difficili da sfruttare ma potrebbero permettere un'elevazione dei privilege o una perdita di dati;
- **Medio**: le vulnerabilità di questo tipo dovrebbero essere affrontate tempestivamente. Sfruttarle è più difficile e richiede il social engineering o particolari circostanze;
- **Basso**: queste vulnerabilità devono essere affrontate in un secondo momento. Offrono pochissime opportunità o informazioni a un utente malintenzionato e potrebbero non rappresentare una minaccia reale.





5. Detailed Summary

Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)

Sinossi:

Il web server è affetto da una vulnerabilità di remote code execution (RCE).

Descrizione:

Il web server è affetto da una vulnerabilità di remote code execution tramite una falla nella libreria Apache Log4j. La vulnerabilità è dovuta all'elaborazione dell'input non sanificato inviato a una funzione di registrazione. Un attaccante remoto e non autenticato può sfruttare questa vulnerabilità e tramite una richiesta web eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Soluzione:

Aggiornare la libreria Apache Logv4j alla versione 2.15.0 o successive, oppure applicazione la mitigazione fornita dal vendor. L'aggiornamento alle versioni più recenti della libreria Apache Log4j è altamente consigliato.

Rischio:

Critico

CVSS v3.0 Base Score:

10.0

Riferimenti:

CVE-2021-44228 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)

Sinossi:

La versione di Apache Log4j utilizzata dal server è affetta da una vulnerabilità di remote code execution (RCE).

Descrizione:

È presente una vulnerabilità di remote code execution nella libreria Apache Log4j < 2.15.0 dovuta ad insufficienti protezioni sulle sostituzioni di lookup dei messaggi quando l'utente controlla l'input. Un attaccante remoto e non autenticato può sfruttare questa vulnerabilità e tramite una richiesta web eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Soluzione:

Aggiornare ad Apache Logv4j alla versione 2.15.0 o successive, oppure applicazione la mitigazione fornita dal vendor. L'aggiornamento alle versioni più recenti di Apache Log4j è altamente consigliato.

Rischio:

Critico

CVSS v3.0 Base Score:

10.0

Riferimenti:

CVE-2021-44228 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)

Sinossi:

La versione di Apache Log4j utilizzata dal server è affetta da una vulnerabilità di remote code execution (RCE).

Descrizione:

È presente una vulnerabilità di remote code execution in Apache Log4j < 2.15.0 a causa di insufficienti protezioni sulle sostituzioni di lookup dei messaggi quando l'utente controlla l'input. Un attaccante remoto può sfruttare questa vulnerabilità tramite una richiesta web per eseguire codice arbitrario con i permessi del processo Java in esecuzione.

Soluzione:

Aggiornare ad Apache Logv4j alla versione 2.15.0 o successive, oppure applicazione la mitigazione fornita dal vendor. L'aggiornamento alle versioni più recenti di Apache Log4j è altamente consigliato.

Rischio:

Critico

CVSS v3.0 Base Score:

10.0

Riferimenti:

CVE-2021-44228 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Apache Log4Shell RCE detection via callback correlation (Direct Check SSH)

Sinossi:

Il servizio SSH consente remote code execution tramite Log4Shell.

Descrizione:

SSH in sé non è vulnerabile a Log4Shell; tuttavia, siccome l'host può eseguire SSH, il server SSH potrebbe essere potenzialmente colpito se tenta di registrare i dati tramite una libreria Log4j vulnerabile.

Soluzione:

Aggiornare ad Apache Logv4j alla versione 2.16.0 o successive, oppure applicazione la mitigazione fornita dal vendor. L'aggiornamento alle versioni più recenti di Apache Log4j è altamente consigliato.

Rischio:

Critico

CVSS v3.0 Base Score:

10.0

Riferimenti:

CVE-2021-44228 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2022-23795

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Una riga utente non è vincolata da un meccanismo di autenticazione specifico che, in circostanze molto particolari, può consentire l'acquisizione di un account.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Critico

CVSS v3.0 Base Score:

9.8

Riferimenti:

CVE-2022-23795 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23795
https://developer.joomla.org/security-centre/872-20220303-core-user-row-are

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2022-23797

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Un filtraggio inadeguato degli ID selezionati in una richiesta potrebbe portare a una possibile iniezione SQL.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Critico

CVSS v3.0 Base Score:

9.8

Riferimenti:

CVE-2022-23797 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23797
https://developer.joomla.org/security-centre/874-20220305-core-inadequate-f

Apache Log4Shell Bypass Remote Code Execution (RCE)

Sinossi:

La versione della libreria Apache Log4j utilizzata dal server è affetta da una vulnerabilità di remote code execution (RCE).

Descrizione:

È presente una vulnerabilità di remote code execution nella libreria Apache Log4j < 2.16.0 dovuta ad insufficienti protezioni sulle sostituzioni di lookup dei messaggi quando l'utente controlla l'input. Un attaccante remoto e non autenticato può sfruttare questa vulnerabilità e tramite una richiesta web eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Soluzione:

Aggiornare la libreria Apache Logv4j alla versione 2.16.0 o successive, oppure applicazione la mitigazione fornita dal vendor. L'aggiornamento alle versioni più recenti della libreria Apache Log4j è altamente consigliato.

Rischio:

Critico

CVSS v3.0 Base Score:

9.0

Riferimenti:

CVE-2021-45046 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046

NodeJS System Information Library Command Injection

Sinossi:

Il server contiene una libreria di un framework per applicazioni web che è affetta da una vulnerabilità di remote command injection.

Descrizione:

Sul server è presente la System Informazion Library per NodeJS, ovvero una raccolta oper source di funzioni per il recupero di informazioni dettagliate sul sistema, hardware e sistema operativo. La versione installate è precedente alla versione 5.3.1. Nelle versioni precedenti alla 5.3.1 è presente una vulnerabilità di tipo command injection.

Soluzione:

Aggiornare la libreria System Information alla versione 5.3.1 o successive.

Rischio:

Alto

CVSS v3.0 Base Score:

8.8

Riferimenti:

CVE-2021-21315 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21315

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2022-23793

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

L'estrazione di un pacchetto .tar appositamente creato potrebbe comportare la scrittura di file al di fuori del percorso previsto.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Alto

CVSS v3.0 Base Score:

7.5

Riferimenti:

CVE-2022-23793 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23793
https://developer.joomla.org/security-centre/870-20220301-core-zip-slip-wit

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26036

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

La mancata convalida dell'input potrebbe causare la rottura della tabella dei gruppi di utenti.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Alto

CVSS v3.0 Base Score:

7.5

Riferimenti:

CVE-2021-26036 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26036

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26038

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

L'azione di installazione in com_installer manca dei controlli ACL codificati per i superutenti. Un sistema predefinito non è interessato perché l'ACL predefinita per com_installer è già limitata ai superutenti.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Alto

CVSS v3.0 Base Score:

7.5

Riferimenti:

CVE-2021-26038 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26038

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26033

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Un controllo mancante del token causa una vulnerabilità CSRF nell'endpoint di riordino AJAX.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

6.5

Riferimenti:

CVE-2021-26033 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26033
https://developer.joomla.org/security-centre/853-20210502-core-csrf-in-ajax

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26034

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Un controllo mancante del token causa una vulnerabilità CSRF negli endpoint di download dei dati in com_banners e com_sysinfo.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

6.5

Riferimenti:

CVE-2021-26034 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26034
https://developer.joomla.org/security-centre/854-20210503-core-csrf-in-data

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2022-23796

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

La mancata convalida dell'input potrebbe consentire un attacco XSS utilizzando com_fields.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

6.1

Riferimenti:

CVE-2022-23796 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23796
https://developer.joomla.org/security-centre/873-20220304-core-missing-inpu

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26035

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

L'escape inadeguato nel campo delle regole dell'API JForm porta a una vulnerabilità XSS.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

6.1

Riferimenti:

CVE-2021-26035 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26035

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26039

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

L'escape inadeguato nella vista imagelist di com_media porta a una vulnerabilità XSS.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

6.1

Riferimenti:

CVE-2021-26039 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26039

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26030

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Un escape inadeguato consente attacchi XSS utilizzando il parametro logo dei modelli predefiniti nella pagina di errore.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

6.1

Riferimenti:

CVE-2021-26030 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26030
https://developer.joomla.org/security-centre/850-20210401-core-escape-xss-i

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2022-23798

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Una convalida inadeguata degli URL potrebbe portare a un controllo non valido se un URL di reindirizzamento è interno o meno.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

6.1

Riferimenti:

CVE-2022-23798 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23798
https://developer.joomla.org/security-centre/875-20220306-core-inadequate-v

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26032

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Mancava l'HTML nell'elenco dei blocchi eseguibili di MediaHelper::canUpload, il che portava a vettori di attacco XSS.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

6.1

Riferimenti:

CVE-2021-26032 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26032
https://developer.joomla.org/security-centre/852-20210501-core-adding-html

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2022-23794

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Il caricamento di un nome di file il cui nome è eccessivamente lungo causa un errore. Questo errore fa apparire una schermata con il percorso del codice sorgente della web application.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

5.3

Riferimenti:

CVE-2022-23794 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23794
https://developer.joomla.org/security-centre/871-20220302-core-path-disclos

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26037

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Le funzioni CMS non terminano correttamente le sessioni utente esistenti quando la password di un utente viene cambiato o l'utente viene bloccato.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

5.3

Riferimenti:

CVE-2021-26037 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26037

Joomla! 2.5.0 - 3.10.6, 4.0.0 - 4.1.0 CVE-2021-26031

Sinossi:

Le versioni di Joomla! Dalla 2.5.0 alla 3.10.6 e dalla 4.0.0 alla 4.1.0 presentano molteplici vulnerabilità.

Descrizione:

Filtri inadeguati sulle impostazioni del modulo layout potrebbero causare un LFI.

Soluzione:

Aggiornare Joomla! Alle versioni 3.10.7, 4.1.1 o successive.

Rischio:

Medio

CVSS v3.0 Base Score:

5.3

Riferimenti:

CVE-2021-26031 https://nvd.nist.gov/vuln/detail/CVE-2021-26031
https://developer.joomla.org/security-centre/851-20210402-core-inadequate-f

6. References

[1] **HarryPotter:Nagini** https://www.vulnhub.com/entry/harrypotter-nagini,689/

[2] **Joomla – Security Centre** https://developer.joomla.org/security-centre/

[3] **CVE Mitre** https://cve.mitre.org/index.html