VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Settimanale

12/10/2026 - 19/10/2026

Generato il: **19/10/2026 06:27**

Piattaforma Avanzata di Cyber Threat Intelligence

https://vulnx.it | Studio Consi

Chi Siamo

Studio Consi è un'azienda specializzata in **cybersecurity** e **consulenza aziendale**, che offre soluzioni avanzate per la valutazione di sicurezza informatica e consulenza per l'implementazione di strategie di protezione e gestione dei rischi.

Vieni a scoprirci

Servizi Offerti

OSINT

Raccolta e analisi di informazioni da fonti aperte per identificare minacce e vulnerabilità esposte.

Formazione

Programmi di formazione specialistica per tecnici IT e percorsi di awareness per utenti finali.

Vulnerability Assessment

Valutazione sistematica delle vulnerabilità presenti nei sistemi informativi.

Malware & Phishing Simulations

Campagne di avanzate e targettizzate per la sensibilizzazione attraverso simulazioni controllate.

Penetration Testing

Test di penetrazione avanzati per simulare attacchi reali.

Consulenza UNI EN ISO

Supporto per certificazioni UNI EN ISO 27001, 9001, 45001, 17020, 17065, IATF 16949:2016 e Regolamento MOCA.

Quality of Service SOC

Verifica dell'effettiva capacità di rilevamento e risposta del Security Operations Center (SOC) attraverso test mirati.

Consulenza Cybersecurity e Data Protection

Advisory strategico e conformità normativa NIS2, GDPR e altre regolamentazioni pertinenti.

Sonar

Studio Consi ha sviluppato Sonar, un innovativo **Assets Inventory & Network Scanner agentless**, una soluzione tecnologica avanzata per la gestione e il monitoraggio continuo delle infrastrutture IT.

- Pattugliamento continuo della rete
- Monitoraggio in tempo reale
- Identificazione automatica nuovi asset
- Rilevamento vulnerabilità (CVE/KEV/EPSS)
- Inventario automatizzato
- Modalità agentless (non invasiva)
- Alert proattivi
- Dashboard centralizzata

Registrati gratuitamente

Indice

1 Sommario Esecutivo **4**
1.1 Statistiche del Periodo 4
1.2 Panoramica Database (Storico Completo) 5

2 Note Metodologiche **7**

3 Analisi delle Debolezze (CWE) **8**
3.1 Distribuzione CWE 8
3.2 Analisi Approfondita delle Debolezze (CWE) 8
3.3 CVE del Periodo Analizzato 10

4 Vulnerabilità Critiche **47**

5 Top 3 Minacce della Settimana **47**
5.1 EPSS Elevato (>95%) 48
5.2 Raccomandazioni 49
5.3 Risorse Aggiuntive 49

1 Sommario Esecutivo

INDICATORE DI RISCHIO SETTIMANALE

ALTO

Rilevate 350 vulnerabilità critiche e 9 exploit attivi.

Metrica	Valore
Totale CVE	**4860**
Critiche	**350**
Alte	**2245**
EPSS >50%	**0**
KEV	**9**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	**4,856**	–
CVE Modificate	17,474	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	**350**	7.5%
Alte (7.0-8.9)	**2245**	47.9%
Medie (4.0-6.9)	1953	41.7%
Basse (0.1-3.9)	140	3.0%
Indicatori di Rischio		
KEV (Exploit Attivi)	**9**	0.2%
EPSS Elevato (>50%)	0	0.0%

Queste statistiche si riferiscono esclusivamente alle vulnerabilità pubblicate o modificate nel periodo analizzato, mentre i totali del database rappresentano l'intero storico.

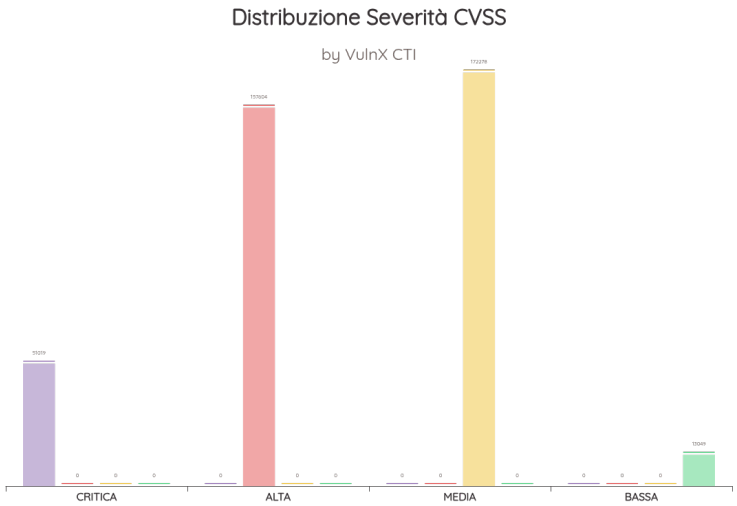
1.2 Panoramica Database (Storico Completo)

Statistiche complete del database storico su tutte le CVE mai pubblicate:

- **CVE Totali nel Database:** 409,174
- **KEV Totali (Vulnerabilità con Exploit Noti):** 1,750
- **CWE Totali Catalogate:** 969
- **CPE Totali Monitorati:** 2,518,261

Severità	Conteggio	Percentuale
CRITICA	51,019	13.0%
ALTA	157,604	40.0%
MEDIA	172,278	43.7%
BASSA	13,049	3.3%

Tabella 1: *Distribuzione per Severità*




Evoluzione Temporale delle CVE
by VulnX CTI
CVE
80,000
60,000
40,000
20,000
0
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026

2 Note Metodologiche

Questo report è stato generato automaticamente utilizzando i dati della piattaforma **VulnX**. I dati includono:

- **Vulnerabilità CVE** dal database MITRE, NVD e EUVD
- **Known Exploited Vulnerabilities (KEV)** da CISA
- **Punteggi CVSS** v2, v3.0, v3.1 e v4.0
- **Punteggi EPSS** (Exploit Prediction Scoring System)
- **Mappature CWE, CAPEC e MITRE ATT&CK** per analisi delle debolezze

Utilizzo dell'Intelligenza Artificiale: Le sezioni "Cosa può succedere?" e le raccomandazioni di mitigazione presenti nel report sono generate automaticamente tramite modelli di intelligenza artificiale per fornire un'analisi contestualizzata delle vulnerabilità. Si raccomanda di validare le informazioni con personale tecnico specializzato e adattarle al proprio contesto operativo.

3 Analisi delle Debolezze (CWE)

3.1 Distribuzione CWE

Il seguente grafico radar mostra i tipi di debolezza (CWE) più comuni identificati in questo periodo:

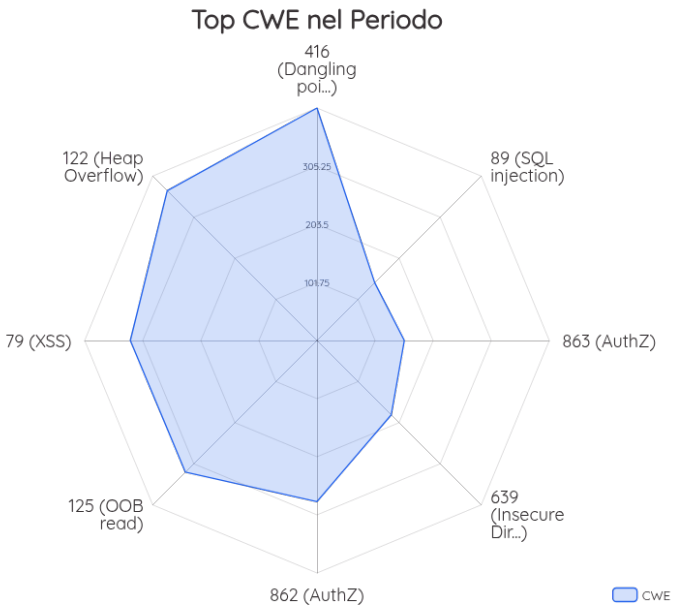


Figura 1: *Distribuzione Top CWE - Grafico Radar*

3.2 Analisi Approfondita delle Debolezze (CWE)

Le debolezze più comuni con raccomandazioni di difesa.

79

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

▶ **Occorrenze:** 327

862

Missing Authorization

▶ **Occorrenze:** 282

639

Authorization Bypass Through User-Controlled Key

▶ Occorrenze: 184

22

Improper Limitation of a Pathname to a Restricted Directory (’Path Traversal’)

▶ Occorrenze: 119

94

Improper Control of Generation of Code (’Code Injection’)

▶ Occorrenze: 91

502

Deserialization of Untrusted Data

▶ Occorrenze: 46

3.3 CVE del Periodo Analizzato

Trovate **4856** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **25** CVE:

CVE-2026-95182 - CVSS 10.0 (CRITICA)

Un percorso di ricerca non affidabile in DeepSeek Harness (dsh) commit c291e796 consente agli attaccanti di eseguire codice arbitrario tramite la fornitura e l'apertura di file eseguibili manipolati al posto di contenuti legittimi.

Descrizione Originale (EN): An untrusted search path in DeepSeek Harness (dsh) commit c291e796 allows attackers to execute arbitrary code via supplying and opening crafted executable files in place of legitimate content.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** changed
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

426: **Untrusted Search Path**

Probabilità di Sfruttamento: high

Termini Alternativi: Untrusted Path

Approfondisci su VulnX

CVE-2026-94169 - CVSS 10.0 (CRITICA)

Vulnerabilità di Controllo Improprio della Generazione di Codice ('Code Injection') in Theme-one The Grid the-grid consente Command Injection. Questo problema riguarda The Grid: dalla versione n/a fino alla 2.8.1.

Descrizione Originale (EN): Improper Control of Generation of Code ('Code Injection') vulnerability in Theme-one The Grid the-grid allows Command Injection.This issue affects The Grid: from n/a through 2.8.1.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.98% (Percentile: 0.62)
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** changed
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

94: **Improper Control of Generation of Code ('Code Injection')**

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Approfondisci su VulnX

CVE-2026-85746 - CVSS 9.9 (CRITICA)

Il server MariaDB è una fork sviluppata dalla comunità di MySQL. Dalla versione 10.6.1 fino alla 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3 e 13.0.2, ST_AsText può scrivere oltre il buffer di output allocato durante la conversione di GeometryCollections profondamente annidate, poiché la serializzazione ricorsiva in WKT non tiene conto dei byte consumati né riserva uno spazio sufficiente. Un attaccante remoto con privilegi bassi può inviare un oggetto GIS appositamente creato per corrompere la memoria e potenzialmente ottenere l'esecuzione di codice quando combinato con un'altra vulnerabilità. Questo problema è stato risolto nelle versioni 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3 e 13.0.2.

Descrizione Originale (EN): MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, ST_AsText can write beyond an allocated output buffer when converting deeply nested GeometryCollections because recursive WKT serialization does not account for bytes consumed or reserve sufficient space. A low-privileged remote attacker can submit a specially crafted GIS object to corrupt memory and potentially achieve code execution when combined with another vulnerability. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** low
- **Interazione Utente:** none
- **Ambito:** changed
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

787: **Out-of-bounds Write**

Probabilità di Sfruttamento: high

Termini Alternativi: Memory Corruption

Approfondisci su VulnX

CVE-2026-92262 - CVSS 9.9 (CRITICA)

Il server MariaDB è un fork sviluppato dalla comunità di MySQL. Dalla versione 10.6.1 fino alla 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3 e 13.0.2, il prefisso #mysql50# è soggetto a vulnerabilità perché consente al prefisso #mysql50# di bypassare la codifica del filesystem del nome della tabella normale. Un attaccante può sfruttare questa vulnerabilità creando un nome di tabella con il prefisso #mysql50#, quindi utilizzare un nome di tabella con prefisso #mysql50# per accedere ai file sotto il loro nome legacy non codificato e causare crash, corruzione dei dati, esfiltrazione di dati o esecuzione di codice remoto. Il problema è stato risolto nelle versioni 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3 e 13.0.2.

Descrizione Originale (EN): MariaDB server is a community developed fork of MySQL server. From 10.6.1 until 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, the #mysql50# bypass prefix is affected because it allows the #mysql50# prefix to bypass normal table-name filesystem encoding. An attacker can trigger the issue with a table name using the #mysql50# prefix, then use a #mysql50# table name to access files under their legacy unencoded name and cause crashes, data corruption, data exfiltration, or remote code execution. This issue is fixed in versions 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** low
- **Interazione Utente:** none
- **Ambito:** changed
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

706: **Use of Incorrectly-Resolved Name or Reference**

Approfondisci su VulnX

CVE-2026-85748 - CVSS 9.9 (CRITICA)

Il server MariaDB è una fork sviluppata dalla comunità di MySQL server. Dalla versione 12.3.1 fino alla 12.3.3 e alla 13.0.2, la gestione di SYS_REFCURSOR è compromessa perché la riallocazione dell'array di cursori può lasciare riferimenti obsoleti nel contesto delle routine. Un attaccante con privilegi bassi può aprire un gran numero di SYS_REFCURSOR e successivamente recuperarne uno per innescare un use-after-free che può consentire l'esecuzione di codice remoto quando combinato con un'altra vulnerabilità. Questo problema è stato risolto nelle versioni 12.3.3 e 13.0.2.

Descrizione Originale (EN): MariaDB server is a community developed fork of MySQL server. From 12.3.1 until 12.3.3 and 13.0.2, SYS_REFCURSOR handling is affected because cursor-array reallocation can leave stale references in routine contexts. A low-privileged attacker can open a large number of SYS_REFCURSORs and then fetch one to trigger a use-after-free that can enable remote code execution when combined with another vulnerability. This issue is fixed in versions 12.3.3 and 13.0.2.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** low
- **Interazione Utente:** none
- **Ambito:** changed
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

416: **Use After Free**

Probabilità di Sfruttamento: high

Termini Alternativi: Dangling pointer, UAF, Use-After-Free

Approfondisci su VulnX

CVE-2026-104736 - CVSS 9.8 (CRITICA)

Il plugin LearnPress per WordPress è vulnerabile a PHP Object Injection nelle versioni fino alla 4.4.10 inclusa, attraverso la deserializzazione di input non affidabili provenienti dal parametro di richiesta 'checkout-email' durante l'azione AJAX di checkout. Il valore viene passato tramite sanitize_text_field(), che non rimuove la sintassi degli oggetti serializzati, quindi memorizzato nella tabella delle sessioni di LearnPress e successivamente passato a LP_Helper::maybe_unserialize() → unserialize() (senza restrizioni su allowed_classes) da LP_Session_Handler::get() nelle richieste successive. Ciò rende possibile agli attori malevoli non autenticati iniettare un PHP Object.

Descrizione Originale (EN): The LearnPress plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 4.4.10 via deserialization of untrusted input from the 'checkout-email' request parameter during the checkout AJAX action. The value is passed through sanitize_text_field(), which does not strip serialized object syntax, then stored in the LearnPress session table and later fed to LP_Helper::maybe_unserialize() → unserialize() (without an allowed_classes restriction) by LP_Session_Handler::get() on subsequent requests. This makes it possible for unauthenticated attackers to inject a PHP Object.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	17/10/2026
Modificata:	17/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

502: **Deserialization of Untrusted Data**

Probabilità di Sfruttamento: medium

Termini Alternativi: Marshaling/Marshalling, Unmarshaling/Unmarshalling, Pickling, Unpickling, PHP Object Injection

Approfondisci su VulnX

CVE-2026-111823 - CVSS 9.8 (CRITICA)

Mage OSS fino alla versione 0.9.80, prima di 76c4f46, può procedere con la creazione della sessione incontrando un provider OAuth sconosciuto.

Descrizione Originale (EN): Mage OSS through 0.9.80 before 76c4f46 can proceed with session creation upon encountering an unknown OAuth provider.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	17/10/2026
Modificata:	17/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

390: **Detection of Error Condition Without Action**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-111711 - CVSS 9.8 (CRITICA)

Netcore NR256CN fino alla versione 1.5.140116 presenta una vulnerabilità di overflow dello stack pre-authentication nel metodo user_ok() del web server Boa, che copia i nomi utente Basic-auth tramite chiamate strcpy() non limitate in buffer di stack da 64 byte. Gli attaccanti non autenticati possono inviare un nome utente più lungo di 63 byte a qualsiasi rotta protetta /router/*.cgi per far crashare il processo principale di Boa o potenzialmente eseguire codice arbitrario.

Descrizione Originale (EN): Netcore NR256CN through 1.5.140116 contains a pre-authentication stack overflow vulnerability in the Boa web server's user_ok() function, which copies Basic-auth usernames with unbounded strcpy() calls into 64-byte stack buffers. Unauthenticated attackers can send a username longer than 63 bytes to any protected /router/*.cgi route to crash the main Boa process or potentially execute code.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-111708 - CVSS 9.8 (CRITICA)

WhaTicket Community, tramite il commit cf04795, contiene una vulnerabilità di bypass dell'autenticazione che consente agli attori malevoli non autenticati di registrarsi autonomamente come amministratori tramite POST /auth/signup. Gli attaccanti possono omettere il campo profile o impostarlo su admin, ottenendo gestione utenti, impostazioni e accesso a tutti i ticket, contatti, messaggi e connessioni WhatsApp.

Descrizione Originale (EN): WhaTicket Community through commit cf04795 contains an authentication bypass vulnerability that allows unauthenticated attackers to self-register as administrators via POST /auth/signup. Attackers can omit the profile field or set it to admin, gaining user management, settings, and access to all tickets, contacts, messages, and WhatsApp connections.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

269: **Improper Privilege Management**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-111704 - CVSS 9.8 (CRITICA)

LangChat fino al commit 2a6285a presenta una vulnerabilità di autenticazione mancante che consente agli attaccanti remoti non autenticati di accedere ai controller REST perché nessun interceptor Sa-Token è registrato. Gli attaccanti possono interrogare /api/v1/auth/users per leggere password in testo semplice, recuperare le chiavi API del provider LLM, creare account super-admin e modificare o eliminare dati.

Descrizione Originale (EN): LangChat through commit 2a6285a contains a missing authentication vulnerability that allows unauthenticated remote attackers to access REST controllers because no Sa-Token interceptor is registered. Attackers can query /api/v1/auth/users to read plaintext passwords, retrieve LLM provider API keys, create super-admin accounts, and modify or delete data.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-111693 - CVSS 9.8 (CRITICA)

DataBuff ai-apm-web fino alla versione 0.1.10 presenta una vulnerabilità di credenziali di default hard-coded che consente agli attaccanti non autenticati di ottenere l'accesso come amministratore utilizzando l'account integrato admin/Databuff@123. Gli attaccanti possono inviare una richiesta POST con queste credenziali a /webapi/api/v1/auth/login per ottenere un token di amministratore e accedere a tutte le rotte protette /webapi.

Descrizione Originale (EN): DataBuff ai-apm-web through 0.1.10 contains a hard-coded default credentials vulnerability that allows unauthenticated attackers to gain administrator access using the built-in admin/Databuff@123 account. Attackers can POST these credentials to /webapi/api/v1/auth/login to obtain an administrator token and access all protected /webapi routes.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

1392: **Use of Default Credentials**

Approfondisci su VulnX

CVE-2026-111687 - CVSS 9.8 (CRITICA)

WeRSS (we-mp-rss) fino alla versione 1.5.3 contiene una vulnerabilità di esecuzione di codice remoto che consente agli attaccanti non autenticati di eseguire codice tramite il parametro template dell'endpoint pubblico GET /rss/{feed_id}. Gli attaccanti possono fornire un valore ext non integrato e un template {{=expression}} il cui attraversamento delle sottoclasse dell'oggetto bypassa la lista di negazione di eval per eseguire comandi OS come account del servizio.

Descrizione Originale (EN): WeRSS (we-mp-rss) through 1.5.3 contains a remote code execution vulnerability that allows unauthenticated attackers to run code via the template parameter of the public GET /rss/{feed_id} endpoint. Attackers can supply a non-built-in ext value and a {{=expression}} template whose object-subclass traversal bypasses the eval denylist to run OS commands as the service account.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

95: **Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-111690 - CVSS 9.8 (CRITICA)

Simple Admin Core fino alla versione 1.8.7 presenta una vulnerabilità di bypass dell'autenticazione che consente agli attaccanti non autenticati di falsificare token di super amministratore utilizzando l'Auth.AccessSecret hard-coded in api/etc/core.yaml. Gli attaccanti possono firmare un JWT con il secret pubblico e il claim roleId 001 per ottenere il controllo amministrativo completo su utenti, ruoli, menu, autorità API, configurazioni e token.

Descrizione Originale (EN): Simple Admin Core through 1.8.7 contains an authentication bypass vulnerability that allows unauthenticated attackers to forge super administrator tokens by using the hard-coded Auth.AccessSecret in api/etc/core.yaml. Attackers can sign a JWT with the public secret and roleId claim 001 to gain full administrative control over users, roles, menus, API authorities, configuration and tokens.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

321: **Use of Hard-coded Cryptographic Key**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-111692 - CVSS 9.8 (CRITICA)

DataBuff ai-apm-web fino alla versione 0.1.10 presenta una vulnerabilità di bypass dell'autenticazione che consente agli attaccanti non autenticati di falsificare token di sessione amministrativa utilizzando il segreto HMAC hardcoded in JwtTokenService. Gli attaccanti possono firmare un payload di tipo admin con una scadenza futura utilizzando il default dev-secret per ottenere un accesso amministrativo completo alle rotte protette /webapi, inclusa l'API di query Doris SQL.

Descrizione Originale (EN): DataBuff ai-apm-web through 0.1.10 contains an authentication bypass vulnerability that allows unauthenticated attackers to forge admin session tokens by using the hardcoded HMAC secret in JwtTokenService. Attackers can sign a payload of admin and a future expiry with the default dev-secret to gain full administrative access to protected /webapi routes, including the Doris SQL query API.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

321: **Use of Hard-coded Cryptographic Key**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-111673 - CVSS 9.8 (CRITICA)

IceCMS fino alla versione 4.1.5 presenta una vulnerabilità di autenticazione mancante che consente agli attaccanti non autenticati di modificare, eliminare o disabilitare qualsiasi account poiché /User/** è escluso dal filtro Shiro jwt. Gli attaccanti possono inviare richieste PUT a /User/updateUser per impostare una nuova password e ruolo su qualsiasi userId, inclusi gli amministratori, consentendo il pieno controllo dell'account.

Descrizione Originale (EN): IceCMS through 4.1.5 contains a missing authentication vulnerability that allows unauthenticated attackers to modify, delete, or disable any account because /User/** is excluded from the Shiro jwt filter. Attackers can send PUT requests to /User/updateUser to set a new password and role on any userId, including administrators, enabling full account takeover.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-111641 - CVSS 9.8 (CRITICA)

FastapiAdmin fino alla versione 3.0 presenta una vulnerabilità di bypass dell'autenticazione che consente agli attaccanti non autenticati di ottenere sessioni per qualsiasi utente sfruttando endpoint di auto-login non protetti. Gli attaccanti possono elencare gli utenti tramite /api/v1/auth/auto-login/users, generare un token auto-login per superuser e scambiarlo con una sessione JWT per ottenere il pieno controllo amministrativo.

Descrizione Originale (EN): FastapiAdmin through 3.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to obtain sessions for any user by abusing unprotected auto-login endpoints. Attackers can list users via /api/v1/auth/auto-login/users, mint a superuser auto-login token, and exchange it for a JWT session to gain full administrative control.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-111626 - CVSS 9.8 (CRITICA)

Webreaper Damselfly fino alla versione 4.5.3 presenta una vulnerabilità di bypass dell'autenticazione che consente agli attaccanti non autenticati di accedere a tutte le route /api/* poiché gli attributi di autorizzazione del controller sono commentati. Gli attaccanti possono inviare PUT /api/users con ruoli Admin per creare account amministratore, oppure POST /api/users per reimpostare la password di qualsiasi utente, ottenendo il controllo completo.

Descrizione Originale (EN): Webreaper Damselfly through 4.5.3 contains an authentication bypass vulnerability that allows unauthenticated attackers to access all /api/* routes because controller authorization attributes are commented out. Attackers can send PUT /api/users with Admin roles to create administrator accounts, or POST /api/users to reset any user's password, gaining full control.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-111643 - CVSS 9.8 (CRITICA)

Misaka Danmu Server fino alla versione 2.8.9 presenta una vulnerabilità di bypass dell'autenticazione che consente agli attaccanti non autenticati di scrivere chiavi di configurazione arbitrarie tramite l'endpoint POST /api/ui/config-history/rollback non protetto. Gli attaccanti possono impostare la chiave ipWhitelist sul proprio indirizzo /32, oppure modificare trustedProxies e webhookApiKey, per accedere a ogni endpoint protetto come amministratore.

Descrizione Originale (EN): Misaka Danmu Server through 2.8.9 contains an authentication bypass vulnerability that allows unauthenticated attackers to write arbitrary configuration keys via the unprotected POST /api/ui/config-history/rollback endpoint. Attackers can set the ipWhitelist key to their own /32 address, or alter trustedProxies and webhookApiKey, to access every protected endpoint as the administrator.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-49868 - CVSS 9.8 (CRITICA)

RIOT è un sistema operativo open-source per microcontrollori progettato per dispositivi Internet of Things e altri sistemi embedded. Prima del 2026.07, _parse_reply() in sys/net/application_layer/dhcpv6/client.c omette la validazione della lunghezza minima prima di passare i corpi delle opzioni IA_PD e IA_NA ai parser delle sotto-opzioni. Un server DHCPv6 malintenzionato o compromesso può inviare una REPLY con una lunghezza dell'opzione inferiore alla struttura richiesta, mentre MODULE_DHCPV6_CLIENT_IA_PD è abilitato, causando _parse_ia_pd_option di leggere oltre il corpo dell'opzione, un underflow di size_t, e letture heap out-of-bounds non limitate che possono causare il crash del dispositivo e potenzialmente esporre o corrompere la memoria. Questo problema è stato risolto nella versione 2026.07.

Descrizione Originale (EN): RIOT is an open-source microcontroller operating system designed for Internet of Things devices and other embedded systems. Prior to 2026.07, _parse_reply() in sys/net/application_layer/dhcpv6/client.c omits minimum-length validation before passing IA_PD and IA_NA option bodies to sub-option parsers. A malicious or compromised DHCPv6 server can send a REPLY with an option length smaller than the required structure while MODULE_DHCPV6_CLIENT_IA_PD is enabled, causing _parse_ia_pd_option to read past the option body, size_t underflow, and unbounded out-of-bounds heap reads that can crash the device and may expose or corrupt memory. This issue is fixed in version 2026.07.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

125: **Out-of-bounds Read**

Termini Alternativi: OOB read

191: **Integer Underflow (Wrap or Wraparound)**

Termini Alternativi: Integer underflow

Approfondisci su VulnX

CVE-2026-107617 - CVSS 9.8 (CRITICA)

Un attaccante può utilizzare una credenziale hard-coded per accedere ai dispositivi EseeCloud.

Descrizione Originale (EN): An attacker can use a hard-coded credential to log in to EseeCloud devices.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

798: **Use of Hard-coded Credentials**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-89079 - CVSS 9.8 (CRITICA)

Il plugin Theme My Login per WordPress è vulnerabile a escalation dei privilegi tramite account takeover nelle versioni fino, e inclusa, 7.2.1. Ciò è dovuto al fatto che il plugin non valida correttamente l'identità dell'utente prima di aggiornare la sua password. Questo rende possibile agli attaccanti non autenticati modificare le password di utenti arbitrari in configurazioni multi-site in determinate configurazioni.

Descrizione Originale (EN): The Theme My Login plugin for WordPress is vulnerable to privilege escalation via account takeover in versions up to, and including, 7.2.1. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords on multi-site setups in certain configurations.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.29% (Percentile: 0.21)
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

269: **Improper Privilege Management**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-104730 - CVSS 9.8 (CRITICA)

The Sunshine Photo Cart – Client Photo Gallery & Photo Proofing for Photographers plugin for WordPress è vulnerabile a PHP Object Injection in tutte le versioni fino alla 3.7.4 inclusa, tramite deserializzazione di input non affidabili. Ciò rende possibile per gli attaccanti non autenticati iniettare un PHP Object. Non è presente una catena POP nota nel software vulnerabile, il che significa che questa vulnerabilità non ha impatto a meno che non sia installato sul sito un altro plugin o tema contenente una catena POP. Se una catena POP è presente tramite un plugin o tema aggiuntivo installato sul sistema target, potrebbe consentire all'attaccante di eseguire azioni come eliminare file arbitrari, recuperare dati sensibili o eseguire codice, a seconda della catena POP presente. Se una catena POP è presente tramite un plugin o tema aggiuntivo installato sul sistema target, l'attaccante può memorizzare il payload dannoso in modo non autenticato tramite la pagina pubblica dei preferiti e attivare la deserializzazione visualizzando qualsiasi immagine in una galleria non visualizzabile o privata.

Descrizione Originale (EN): The Sunshine Photo Cart – Client Photo Gallery & Photo Proofing for Photographers plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.7.4 via deserialization of untrusted input . This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. If a POP chain is present via an additional plugin or theme installed on the target system, the attacker can store the malicious payload unauthenticated via the public favorites page and trigger deserialization by viewing any image in a non-viewable or private gallery.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.51% (Percentile: 0.42)
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

502: **Deserialization of Untrusted Data**

Probabilità di Sfruttamento: medium

Termini Alternativi: Marshaling/Marshalling, Unmarshaling/Unmarshalling, Pickling, Unpickling, PHP Object Injection

Approfondisci su VulnX

CVE-2026-103768 - CVSS 9.8 (CRITICA)

Il plugin ELEX WordPress HelpDesk & Customer Ticketing System per WordPress è vulnerabile a Upload di File Arbitrario in tutte le versioni fino alla 3.3.7 inclusa tramite la funzione initMailPart. Ciò è dovuto a una validazione insufficiente del tipo di file durante il salvataggio degli allegati email IMAP. Questo rende possibile agli attaccanti non autenticati caricare file potenzialmente eseguibili, consentendo così l'esecuzione di codice remoto.

Descrizione Originale (EN): The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 3.3.7 via the initMailPart function. This is due to insufficient file type validation when saving IMAP email attachments. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.58% (Percentile: 0.46)
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

434: **Unrestricted Upload of File with Dangerous Type**

Probabilità di Sfruttamento: medium

Termini Alternativi: Unrestricted File Upload

Approfondisci su VulnX

CVE-2026-109515 - CVSS 9.8 (CRITICA)

Il plugin MailOptin – Popup, Optin Forms & Email Newsletters for Mailchimp, HubSpot, AWeber Etc. per WordPress è vulnerabile a escalation dei privilegi in tutte le versioni fino alla 1.2.78.6 inclusa. Ciò è dovuto al fatto che l'endpoint 'subscribe_to_email_list' accetta un parametro 'optin_data[form_custom_field_mappings]' fornito dall'attaccante senza alcuna validazione allow-list sui valori di destinazione, consentendo alla mappatura controllata dall'attaccante di sovrascrivere la mappatura salvata dall'amministratore e di passare nomi di colonne arbitrari di 'wp_users' — inclusi 'ID' e 'user_pass' — direttamente in 'wp_insert_user()' tramite la funzione 'subscribe()'. Questo rende possibile agli attaccanti non autenticati forzare 'wp_insert_user()' in modalità UPDATE su qualsiasi account esistente, fornendo un 'ID' numerico dell'utente target, sovrascrivendo la password di quell'account con un valore pre-hashato a loro scelta, e di conseguenza prendere il controllo di qualsiasi account utente di WordPress — inclusi gli amministratori — portando a una compromissione completa del sito. L'exploit richiede che un modulo di registrazione utente di WordPress con opt-in sia pubblicato da qualche parte sul sito, anche se l'UUID del modulo è visibile nel codice sorgente della pagina e non è richiesta autenticazione, nonce o verifica di capability per raggiungere l'endpoint vulnerabile.

Descrizione Originale (EN): The MailOptin – Popup, Optin Forms & Email Newsletters for Mailchimp, HubSpot, AWeber Etc. plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2.78.6 This is due to the 'subscribe_to_email_list' endpoint accepting an attacker-supplied 'optin_data[form_custom_field_mappings]' parameter without any allow-list validation on destination keys, allowing the attacker-controlled mapping to override the administrator's saved mapping and pass arbitrary 'wp_users' column names — including 'ID' and 'user_pass' — directly into 'wp_insert_user()' via the 'subscribe()' function. This makes it possible for unauthenticated attackers to force 'wp_insert_user()' into UPDATE mode on any existing account by supplying a target user's numeric 'ID', overwrite that account's password with a pre-hashed value of their choosing, and thereby take over any WordPress user account — including administrators — leading to full site compromise. Exploitation requires that a WordPress User Registration opt-in form is published somewhere on the site, though the form's UUID is visible in page source and no authentication, nonce, or capability check is required to reach the vulnerable endpoint.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.44% (Percentile: 0.37)
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

269: **Improper Privilege Management**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-109219 - CVSS 9.8 (CRITICA)

Il plugin Mang Board per WordPress è vulnerabile a Vulnerabilità di Upload Arbitrario di File in tutte le versioni fino alla 2.4.4 inclusa tramite la funzione mbw_file_upload. Ciò è dovuto alla mancanza di convalida dell'estensione del file sul parametro image_path fornito dall'attaccante, il cui nome di file derivato da basename aggira la whitelist delle estensioni applicata solo al parametro separato file_name. Questo rende possibile per attaccanti non autenticati caricare file potenzialmente eseguibili, consentendo l'esecuzione di codice remoto. Lo sfruttamento richiede che il board sia configurato per permettere post da ospiti, modalità predefinita del plugin; il nonce necessario viene stampato su ogni pagina pubblica del board, rendendolo leggibile da qualsiasi visitatore non autenticato senza login WordPress.

Descrizione Originale (EN): The Mang Board plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.4.4 via the mbw_file_upload function. This is due to missing file extension validation on the attacker-supplied image_path parameter, whose basename-derived file name bypasses the extension allowlist applied only to the separate file_name parameter. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. Exploitation requires the board to be configured to allow guest posts, which is the plugin's default mode; the required nonce is printed on every public board page, making it readable by any unauthenticated visitor without a WordPress login.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.69% (Percentile: 0.52)
Pubblicata:	16/10/2026
Modificata:	16/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

Stato della Patch: Patch Non Segnalata dal NVD - Verificare Canali Ufficiali del Vendor

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

434: **Unrestricted Upload of File with Dangerous Type**

Probabilità di Sfruttamento: medium

Termini Alternativi: Unrestricted File Upload

Approfondisci su VulnX

4 Vulnerabilità Critiche

5 Top 3 Minacce della Settimana

Le tre vulnerabilità più critiche basate su CVSS, EPSS e contesto degli exploit.

Minaccia #1: CVE-2026-105134 KEV

CVSS: 10.0/10 **EPSS:** 4.8% **Target:** Unknown **Rischio:** 7.1/10

Minaccia #2: CVE-2026-104935 KEV

CVSS: 8.6/10 **EPSS:** 26.0% **Target:** Unknown **Rischio:** 6.9/10

Minaccia #3: CVE-2026-76519 KEV

CVSS: 9.8/10 **EPSS:** 1.6% **Target:** Unknown **Rischio:** 6.9/10

5.1 EPSS Elevato (>95%)

Non sono state identificate vulnerabilità con un EPSS > 95% nel periodo analizzato.

5.2 Raccomandazioni

1. **Applicare patch** per tutte le vulnerabilità con **EPSS > 50%**
2. **Monitorare** le CVE aggiunte di recente al catalogo **CISA KEV**
3. Non **Concentrarsi** solamente sulle vulnerabilità di severità **CRITICA** e **ALTA**
4. **Implementare** monitoraggio continuo tramite **VulnX**

5.3 Risorse Aggiuntive

- **Database CVE:** https://vulnx.it/cve/
- **Database KEV:** https://vulnx.it/kev/
- **Catalogo CWE:** https://vulnx.it/cwe/
- **CAPEC:** https://vulnx.it/capec/

VulnX

Piattaforma Avanzata di Cyber Threat Intelligence in lingua italiana

https://vulnx.it

Studio Consi