VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Mensile

31/01/2026 - 02/03/2026

Generato il: **02/03/2026 12:21**

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

INDICATORE DI RISCHIO MENSILE

ALTO

Riepilogo Settimanale Livello di Minaccia:
Questa settimana sono state identificate 4916 nuove CVE, di cui 492 classificate come critiche e 1641 come ad alta gravità. Si evidenzia la presenza di 28 vulnerabilità aggiunte al catalogo KEV e 9 con un punteggio EPSS superiore al 50%, indicando un'elevata probabilità di exploit. **Azione Consigliata:** Si raccomanda di prioritizzare la mitigazione delle 28 CVE presenti nel catalogo KEV e delle 9 con EPSS >50% a causa del loro elevato rischio di sfruttamento attivo. È inoltre fondamentale monitorare attentamente le vulnerabilità critiche e ad alta gravità per potenziali exploit.

Metrica	Valore
Totale CVE	**4916**
Critiche	**492**
Alte	**1641**
EPSS >50%	**9**
KEV	**28**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	4,907	–
CVE Modificate	7,595	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	492	11.2%
Alte (7.0-8.9)	1641	37.3%
Medie (4.0-6.9)	2020	45.9%
Basse (0.1-3.9)	251	5.7%
Indicatori di Rischio		
KEV (Exploit Attivi)	28	0.6%
EPSS Elevato (>50%)	9	0.2%

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

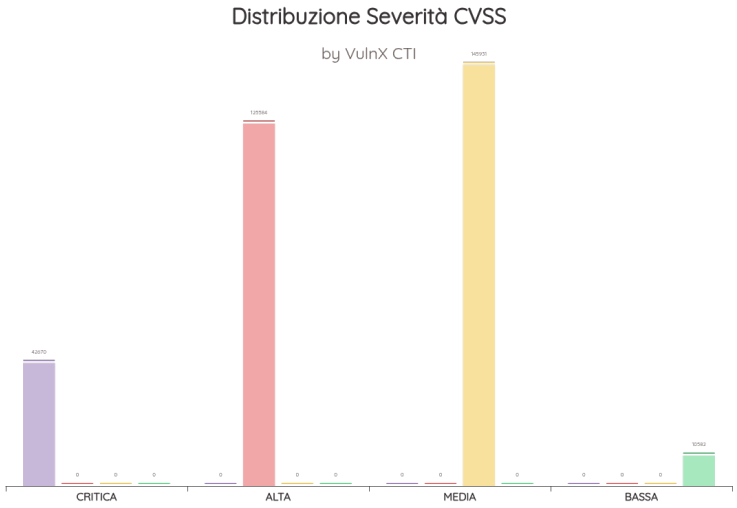
1.2 Panoramica Database (Storico Completo)

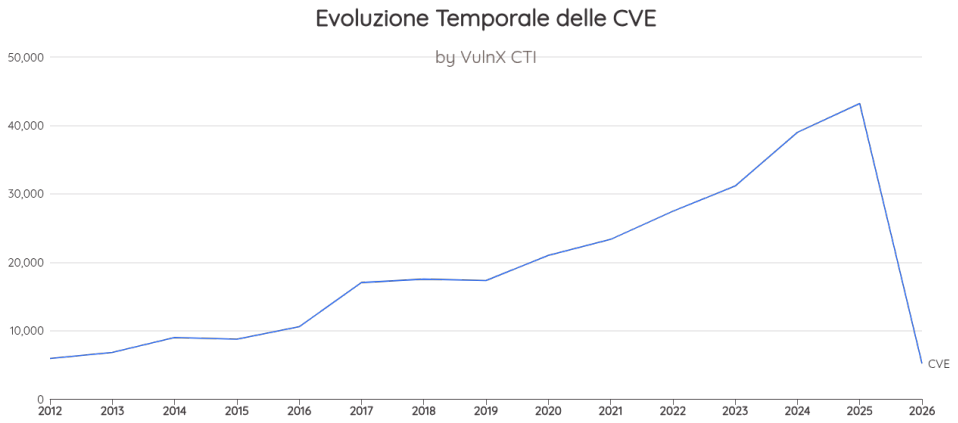
Statistiche complete del database storico su tutte le CVE mai pubblicate:

- **CVE Totali nel Database:** 335,279
- **KEV Totali (Vulnerabilità con Exploit Noti):** 1,531
- **CWE Totali Catalogate:** 969
- **CPE Totali Monitorati:** 2,216,881

Severità	Conteggio	Percentuale
CRITICA	42,670	13.1%
ALTA	125,584	38.7%
MEDIA	145,931	44.9%
BASSA	10,582	3.3%

Tabella 1: *Distribuzione per Severità*


Distribuzione Severità CVSS
by VulnX CTI
CRITICA
ALTA
MEDIA
BASSA


Evoluzione Temporale delle CVE
by VulnX CTI
50,000
40,000
30,000
20,000
10,000
0
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
CVE

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:

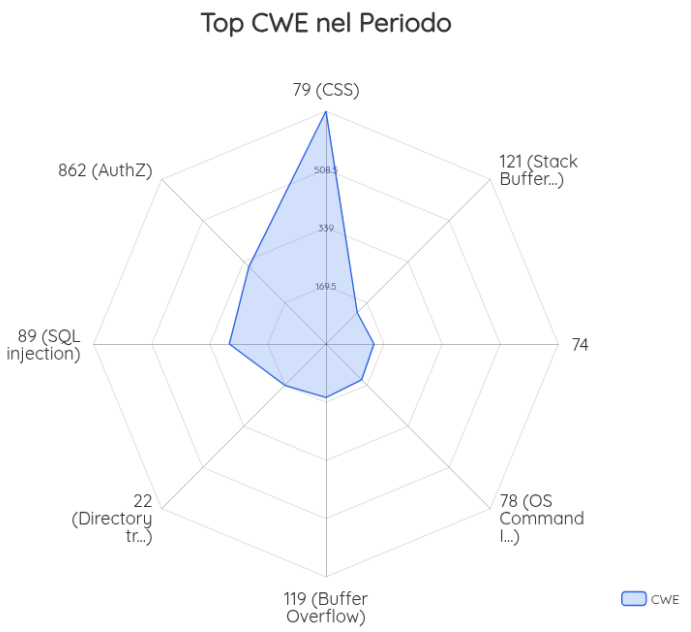


Figura 1: *Distribuzione Top CWE - Grafico Radar*

3.2 Analisi Approfondita delle Debolezze (CWE)

Le debolezze più comuni con raccomandazioni di difesa.

89

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

▶ **Occorrenze:** 282

Raccomandazioni di Difesa

- Ecco 2-3 raccomandazioni specifiche e attuabili per la debolezza CWE-89:
- N/A**Pratiche di Sviluppo:**Implementare l'uso esclusivo di prepared statements o query parametrizzate per tutte le interazioni con il database, evitando la concatenazione di stringhe per costruire query SQL.
- N/A**Strumenti di Sicurezza:**Configurare un Web Application Firewall (WAF) per rilevare e bloccare proattivamente tentativi noti di SQL Injection prima che raggiungano l'applicazione.
- N/A**Configurazioni del Database:**Applicare il principio del minimo privilegio agli account utente del database, concedendo solo le autorizzazioni strettamente necessarie (es. SELECT, INSERT, UPDATE) per le operazioni specifiche richieste dall'applicazione.

119

Improper Restriction of Operations within the Bounds of a Memory Buffer

- **Occorrenze:** 156

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni di difesa specifiche e attuabili per CWE-119:
- N/A**Pratiche di Sviluppo:**Implementare una rigorosa validazione degli input per tutti i dati provenienti da fonti esterne, controllando lunghezza e formato prima dell'elaborazione.
- N/A**Pratiche di Sviluppo:**Adottare funzioni e librerie di gestione della memoria e delle stringhe che includano controlli sui limiti (es. 'snprintf', 'std::string' in C++, linguaggi memory-safe).
- N/A**Configurazioni di Sicurezza:**Abilitare le protezioni a livello di compilatore (es. stack canaries, ASLR, DEP) e del sistema operativo per mitigare gli exploit da buffer overflow.

787

Out-of-bounds Write

▶ **Occorrenze:** 124

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per difendersi da CWE-787 (Out-of-bounds Write):
- N/A**Pratiche di sviluppo:**Implementare una validazione rigorosa degli input e controlli sui limiti (bounds checking) per tutte le operazioni di scrittura in memoria, privilegiando linguaggi o costrutti memory-safe (es. Rust, smart pointers in C++) e funzioni di libreria sicure.
- N/A**Strumenti di sicurezza (SDLC):**Integrare strumenti di sanitizzazione della memoria (es. AddressSanitizer - ASan) nel ciclo di sviluppo e testing per rilevare proattivamente errori di out-of-bounds write prima del deployment.
- N/A**Configurazioni di sistema/compilatore:**Abilitare le protezioni di runtime del compilatore (es. '-fstack-protector') e le funzionalità di sicurezza del sistema operativo come ASLR (Address Space Layout Randomization) e DEP/NX (Data Execution Prevention/No-Execute) per mitigare l'impatto di eventuali exploit.

284

Improper Access Control

▶ **Occorrenze:** 106

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-284 - Improper Access Control:
- N/A**Implementare il principio del privilegio minimo:**Assicurare che utenti e servizi abbiano solo le autorizzazioni strettamente necessarie per svolgere le proprie funzioni.
- N/A**Adottare il controllo degli accessi basato sui ruoli (RBAC):**Progettare e implementare un sistema RBAC per gestire le autorizzazioni in modo granulare e centralizzato, assegnando i permessi ai ruoli anziché direttamente agli utenti.
- N/A**Configurare la segmentazione della rete e firewall:**Isolare i sistemi critici e i dati sensibili tramite segmentazione di rete e applicare regole firewall restrittive che consentano solo il traffico e gli accessi indispensabili.

125

Out-of-bounds Read

- **Occorrenze:** 101

Raccomandazioni di Difesa

- Ecco 2-3 raccomandazioni di difesa specifiche e attuabili per CWE-125 (Out-of-bounds Read):
- N/A**Pratiche di Sviluppo:**Implementare controlli rigorosi sui limiti (boundary checks) per tutti gli accessi a buffer e array, utilizzando funzioni di gestione della memoria sicure (es. 'snprintf', 'strncpy_s') che prevengono letture out-of-bounds.
- N/A**Strumenti di Sicurezza/Configurazioni:**Integrare strumenti di analisi statica del codice (SAST) nelle pipeline CI/CD e adottare sanitizer di memoria (es. AddressSanitizer) nelle fasi di test per rilevare proattivamente vulnerabilità di out-of-bounds read.
- N/A**Controlli di Rete (per applicazioni web):**Configurare regole WAF (Web Application Firewall) per una validazione e sanificazione stringente degli input, in particolare per lunghezza e tipo di dati, al fine di mitigare attacchi che sfruttano input malformati per causare letture out-of-bounds.

416

Use After Free

▶ **Occorrenze:** 75

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-416 (Use After Free):
- N/A**Pratiche di Sviluppo:**Adottare l'uso di smart pointer (es. 'std::unique_ptr', 'std::shared_ptr' in C++) o preferire linguaggi con gestione automatica della memoria (es. Rust, Go, Java) per prevenire errori di deallocazione.
- N/A**Strumenti di Sicurezza:**Integrare e configurare sanitizers di memoria (es. AddressSanitizer - ASan) nelle fasi di sviluppo e test per rilevare e diagnosticare vulnerabilità Use After Free a runtime.
- N/A**Controlli di Sviluppo:**Eseguire analisi statica del codice (SAST) regolarmente, configurando le regole per identificare pattern di gestione della memoria a rischio di Use After Free nel ciclo di CI/CD.

3.3 CVE del Periodo Analizzato

Trovate **4907** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **50** CVE:

CVE-2026-28517 - CVSS 9.3 (CRITICA)

openDCIM versione 23.04, fino al commit 4467e9c4, presenta una vulnerabilità di iniezione di comandi OS in report_network_map.php. L'applicazione recupera il parametro di configurazione 'dot' dal database e lo passa direttamente a exec() senza convalida o sanificazione. Se un attaccante riesce a modificare il valore di fac_Config.dot, potrebbero essere eseguiti comandi arbitrari nel contesto del processo del server web.

Descrizione Originale (EN): openDCIM version 23.04, through commit 4467e9c4, contains an OS command injection vulnerability in report_network_map.php. The application retrieves the 'dot' configuration parameter from the database and passes it directly to exec() without validation or sanitation. If an attacker can modify the fac_Config.dot value, arbitrary commands may be executed in the context of the web server process.

Cosa può succedere?
Un attaccante potrebbe eseguire comandi arbitrari sul server web, ottenendo il pieno controllo del sistema. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi critici o alla compromissione completa dell'infrastruttura IT aziendale.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.27% (Percentile: 0.50) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare controlli di accesso rigorosi al database che ospita la configurazione di openDCIM. Assicurarsi che solo gli amministratori autorizzati abbiano permessi di scrittura sulla tabella 'fac_Config', prevenendo modifiche non autorizzate del parametro 'dot' che potrebbero innescare l'iniezione di comandi.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

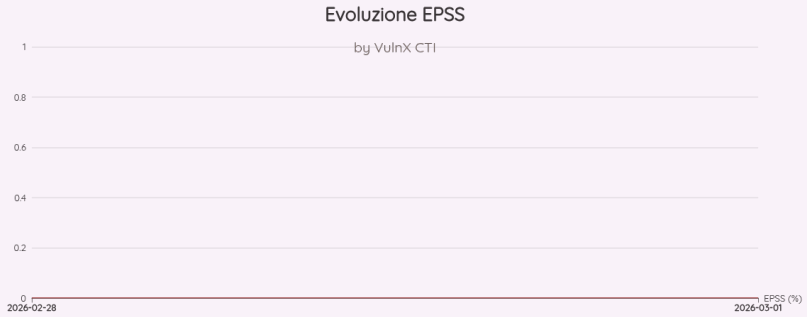
CWE - Common Weakness Enumeration

78: **Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: OS Command Injection, Shell injection, Shell metacharacters

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-2844 - CVSS 9.3 (CRITICA)

Vulnerabilità Missing Authentication for Critical Function in Microchip TimePictra consente la Manipolazione della Configurazione/ambiente. Questo problema riguarda TimePictra: dalla versione 11.0 alla 11.3 SP2.

Descrizione Originale (EN): Missing Authentication for Critical Function vulnerability in Microchip TimePictra allows Configuration/Environment Manipulation.This issue affects TimePictra: from 11.0 through 11.3 SP2.

Cosa può succedere?

Un attaccante può manipolare le configurazioni critiche del sistema TimePictra senza autenticazione, compromettendo gravemente l'integrità operativa. Ciò può causare interruzioni significative dei servizi, perdita di dati o facilitare l'accesso non autorizzato ad altri sistemi aziendali.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.05% (Percentile: 0.15) Disponibili 2 valori storici
Pubblicata:	28/02/2026
Modificata:	28/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare la vulnerabilità, isolate i sistemi Microchip TimePictra interessati in un segmento di rete dedicato e strettamente controllato. Implementate regole firewall restrittive per consentire l'accesso a tali sistemi solo da workstation di gestione autorizzate e per le porte strettamente necessarie. Questo limita significativamente l'esposizione della funzione critica priva di autenticazione a un perimetro di fiducia ridotto.

CVSS Metrics

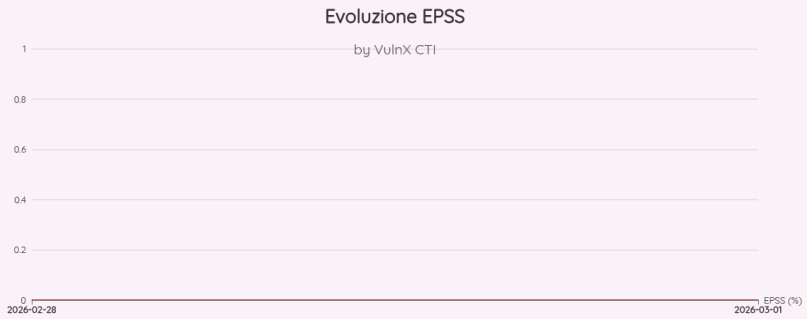
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-3010 - CVSS 9.3 (CRITICA)

Vulnerabilità di Neutralizzazione Impropria dell'Input durante la Generazione di Pagine Web (XSS o 'Cross-site Scripting') in Microchip TimePictra consente Query System for Information. Questo problema riguarda TimePictra: dalle versioni 11.0 fino alla 11.3 SP2.

Descrizione Originale (EN): Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Microchip TimePictra allows Query System for Information.This issue affects TimePictra: from 11.0 through 11.3 SP2.

Cosa può succedere?

Sfruttando questa vulnerabilità, un attaccante potrebbe rubare dati sensibili degli utenti e ottenere accesso non autorizzato ai loro account. Ciò potrebbe compromettere la riservatezza delle informazioni aziendali e portare a ulteriori violazioni dei sistemi.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.05% (Percentile: 0.14) Disponibili 2 valori storici
Pubblicata:	28/02/2026
Modificata:	28/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Data l'assenza di una patch, implementare un Web Application Firewall (WAF) di fronte a Microchip TimePictra. Configurare il WAF con regole robuste per il filtraggio e la neutralizzazione degli input, bloccando attivamente i tentativi di attacco Cross-Site Scripting (XSS) prima che raggiungano l'applicazione.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Termini Alternativi: CSS, DOM-Based XSS / Type 0 XSS, HTML Injection, Reflected XSS / Non-Persistent XSS / Type 1 XSS, Stored XSS / Persistent XSS / Type 2 XSS

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-2584 - CVSS 9.3 (CRITICA)

È stata identificata una vulnerabilità critica di SQL Injection (SQLi) nel modulo di autenticazione del sistema. Un attaccante remoto non autenticato (AV:N/PR:N) può sfruttare questa falla inviando query SQL appositamente formulate tramite l'interfaccia di login. A causa della bassa complessità dell'attacco (AC:L) e dell'assenza di requisiti specifici (AT:N), la vulnerabilità consente una compromissione totale dei dati di configurazione del sistema (VC:H/VI:H). Sebbene la disponibilità del servizio rimanga invariata (VA:N), la violazione può comportare un'esposizione limitata di informazioni sensibili relative a sistemi successivi o interconnessi (SC:L).

Descrizione Originale (EN): A critical SQL Injection (SQLi) vulnerability has been identified in the authentication module of the system. An unauthenticated, remote attacker (AV:N/PR:N) can exploit this flaw by sending specially crafted SQL queries through the login interface. Due to low attack complexity (AC:L) and the absence of specific requirements (AT:N), the vulnerability allows for a total compromise of the system's configuration data (VC:H/VI:H). While the availability of the service remains unaffected (VA:N), the breach may lead to a limited exposure of sensitive information regarding subsequent or interconnected systems (SC:L).

Cosa può succedere?
Un attaccante può facilmente rubare o manipolare tutti i dati di configurazione critici del sistema, ottenendo pieno accesso non autorizzato. Questo comporta una grave perdita di dati sensibili, compromissione dell'integrità del sistema e potenziale interruzione delle operazioni aziendali.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	N/A
Pubblicata:	02/03/2026
Modificata:	02/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare una Web Application Firewall (WAF) di fronte al sistema affetto per filtrare e bloccare proattivamente tentativi di SQL Injection prima che raggiungano l'applicazione. Configurare il WAF con regole robuste per il rilevamento di pattern SQLi specifici e per limitare il traffico anomalo verso il modulo di autenticazione, agendo come controllo compensativo.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

89: **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: SQL injection, SQLi

Approfondisci su VulnX

CVE-2026-28516 - CVSS 9.3 (CRITICA)

openDCIM versione 23.04, fino al commit 4467e9c4, contiene una vulnerabilità di SQL injection in Config::UpdateParameter. I gestori install.php e container-install.php passano input forniti dall'utente direttamente nelle istruzioni SQL utilizzando interpolazione di stringhe senza dichiarazioni preparate o corretta sanificazione degli input. Un utente autenticato può eseguire istruzioni SQL arbitrarie sul database sottostante.

Descrizione Originale (EN): openDCIM version 23.04, through commit 4467e9c4, contains a SQL injection vulnerability in Config::UpdateParameter. The install.php and container-install.php handlers pass user-supplied input directly into SQL statements using string interpolation without prepared statements or proper input sanitation. An authenticated user can execute arbitrary SQL statements against the underlying database.

Cosa può succedere?

Un utente malintenzionato autenticato potrebbe rubare, modificare o cancellare dati sensibili dal database aziendale. Questo porterebbe a gravi violazioni della privacy, interruzioni dei servizi e un potenziale controllo completo del sistema sottostante.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.04% (Percentile: 0.11) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare l'istanza di openDCIM in un segmento di rete dedicato e strettamente controllato, separato da altri sistemi critici. Implementare regole firewall restrittive per consentire l'accesso all'interfaccia di amministrazione solo da indirizzi IP o host specifici e affidabili, preferibilmente tramite una jump box o VPN, riducendo drasticamente la superficie di attacco.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

89: **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: SQL injection, SQLi

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28515 - CVSS 9.3 (CRITICA)

openDCIM versione 23.04, tramite commit 4467e9c4, contiene una vulnerabilità di autorizzazione mancante in install.php e container-install.php. L'installer e l'upgrade handler espongono la funzionalità di configurazione LDAP senza imporre controlli sui ruoli dell'applicazione. Qualsiasi utente autenticato può accedere a questa funzionalità indipendentemente dai privilegi assegnati. In deployment in cui REMOTE_USER è impostato senza un'implementazione di enforcement dell'autenticazione, l'endpoint potrebbe essere accessibile senza credenziali. Ciò consente la modifica non autorizzata della configurazione dell'applicazione.

Descrizione Originale (EN): openDCIM version 23.04, through commit 4467e9c4, contains a missing authorization vulnerability in install.php and container-install.php. The installer and upgrade handler expose LDAP configuration functionality without enforcing application role checks. Any authenticated user can access this functionality regardless of assigned privileges. In deployments where REMOTE_USER is set without authentication enforcement, the endpoint may be accessible without credentials. This allows unauthorized modification of application configuration.

Cosa può succedere?

Qualsiasi utente autenticato, anche con privilegi minimi, può modificare le impostazioni di autenticazione LDAP. Questo permette di creare account amministrativi non autorizzati, accedere a dati sensibili o causare interruzioni gravi ai servizi aziendali.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.12% (Percentile: 0.32) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Configurare un Web Application Firewall (WAF) o un reverse proxy (es. Nginx, Apache) per bloccare l'accesso diretto ai file 'install.php' e 'container-install.php' per tutti gli utenti, ad eccezione di indirizzi IP specifici o di un gruppo ristretto di amministratori. Questo controllo compensativo esterno impedisce agli utenti autenticati non autorizzati di raggiungere e manipolare la configurazione LDAP, mitigando il rischio in assenza di una patch.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

862: **Missing Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28409 - CVSS 10.0 (CRITICA)

WeGIA è un gestore web per istituzioni benefiche. Prima della versione 3.6.5, esisteva una vulnerabilità critica di Remote Code Execution (RCE) nella funzionalità di ripristino del database dell'applicazione WeGIA. Un attaccante con accesso amministrativo (che può essere ottenuto tramite l'Authentication Bypass precedentemente segnalato) può eseguire comandi arbitrari sul sistema operativo del server caricando un file di backup con un nome file appositamente manipolato. La versione 3.6.5 risolve il problema.

Descrizione Originale (EN): WeGIA is a web manager for charitable institutions. Prior to version 3.6.5, a critical Remote Code Execution (RCE) vulnerability exists in the WeGIA application's database restoration functionality. An attacker with administrative access (which can be obtained via the previously reported Authentication Bypass) can execute arbitrary OS commands on the server by uploading a backup file with a specifically crafted filename. Version 3.6.5 fixes the issue.

Cosa può succedere?
Un attaccante potrebbe ottenere il controllo completo del server, permettendo l'esecuzione di comandi arbitrari. Ciò potrebbe causare il furto di dati sensibili, l'interruzione totale dei servizi critici e l'utilizzo del server come base per ulteriori attacchi, con gravi perdite finanziarie e danni alla reputazione aziendale.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.21% (Percentile: 0.44) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare una rigorosa segmentazione di rete per il server che ospita l'applicazione WeGIA, posizionandolo in una zona di rete isolata (ad esempio, una DMZ interna o una subnet dedicata). Limitare l'accesso a questa rete solo alle porte e ai protocolli strettamente indispensabili per il funzionamento dell'applicazione. Questo ridurrà drasticamente la superficie di attacco e frenerà la capacità di movimento laterale di un attaccante all'interno dell'infrastruttura, anche in caso di compromissione del server.

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

78: **Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: OS Command Injection, Shell injection, Shell metacharacters

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-21718 - CVSS 10.0 (CRITICA)

Una vulnerabilità di bypass dell'autenticazione esiste in Copeland XWEB Pro versione 1.12.1 e precedenti, consentendo a qualsiasi attaccante di bypassare il requisito di autenticazione e ottenere l'esecuzione di codice pre-autenticato sul sistema.

Descrizione Originale (EN): An authentication bypass vulnerability exists in Copeland XWEB Pro version 1.12.1 and prior, enabling any attackers to bypass the authentication requirement and achieve pre-authenticated code execution on the system.

Cosa può succedere?

Un attaccante può ottenere il controllo totale del sistema senza autenticazione, eseguendo codice arbitrario. Ciò consente il furto di dati sensibili, l'interruzione dei servizi critici e la potenziale diffusione di malware, con gravi ripercussioni finanziarie e reputazionali per l'azienda.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.07% (Percentile: 0.21) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolate immediatamente il sistema Copeland XWEB Pro in una VLAN o segmento di rete dedicato, applicando regole firewall estremamente restrittive. Consentite l'accesso all'interfaccia di gestione solo da indirizzi IP o sottoreti strettamente autorizzate e monitorate, riducendo al minimo l'esposizione della superficie d'attacco.

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

327: **Use of a Broken or Risky Cryptographic Algorithm**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27613 - CVSS 10.0 (CRITICA)

TinyWeb è un web server (HTTP, HTTPS) scritto in Delphi per Win32. Una vulnerabilità nelle versioni precedenti alla 2.01 consente agli attaccanti remoti non autenticati di bypassare i controlli di sicurezza sui parametri CGI del web server. A seconda della configurazione del server e dell'eseguibile CGI specifico in uso, l'impatto può essere la divulgazione del codice sorgente o l'esecuzione remota di codice (RCE). Chiunque ospiti script CGI (in particolare linguaggi interpretati come PHP) utilizzando versioni vulnerabili di TinyWeb è interessato. Il problema è stato risolto nella versione 2.01. Se l'aggiornamento non è immediatamente possibile, assicurarsi che 'STRICT_CGI_PARAMS' sia abilitato (è definito di default in 'define.inc') e/o non utilizzare eseguibili CGI che accettano nativamente flag pericolosi da riga di comando (come 'php-cgi.exe'). Se si ospita PHP, considerare di posizionare il server dietro un Web Application Firewall (WAF) che blocchi esplicitamente i parametri della query string URL che iniziano con un trattino ('-') o contengono doppi apici codificati ('%22').

Descrizione Originale (EN): TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. A vulnerability in versions prior to 2.01 allows unauthenticated remote attackers to bypass the web server's CGI parameter security controls. Depending on the server configuration and the specific CGI executable in use, the impact is either source code disclosure or remote code execution (RCE). Anyone hosting CGI scripts (particularly interpreted languages like PHP) using vulnerable versions of TinyWeb is impacted. The problem has been patched in version 2.01. If upgrading is not immediately possible, ensure 'STRICT_CGI_PARAMS' is enabled (it is defined by default in 'define.inc') and/or do not use CGI executables that natively accept dangerous command-line flags (such as 'php-cgi.exe'). If hosting PHP, consider placing the server behind a Web Application Firewall (WAF) that explicitly blocks URL query string parameters that begin with a hyphen ('-') or contain encoded double quotes ('%22').

Cosa può succedere?

Gli attaccanti remoti non autenticati potrebbero ottenere il controllo completo del server web. Questo potrebbe portare al furto di dati sensibili, alla compromissione dei sistemi aziendali e all'interruzione dei servizi critici.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.21% (Percentile: 0.43) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un Web Application Firewall (WAF) davanti al server TinyWeb per filtrare e bloccare richieste malevole dirette ai parametri CGI. Configurare il WAF con regole specifiche per rilevare e prevenire tentativi di manipolazione dei parametri o di iniezione di codice, fungendo da ”patch virtuale” per questa vulnerabilità critica e mitigando il rischio di esecuzione remota.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

78: **Improper Neutralization of Special Elements used in an OS Command (’OS Command Injection’)**

Probabilità di Sfruttamento: high

Termini Alternativi: OS Command Injection, Shell injection, Shell metacharacters

---

88: **Improper Neutralization of Argument Delimiters in a Command (’Argument Injection’)**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-2749 - CVSS 9.9 (CRITICA)

Vulnerabilità in Centreon Centreon Open Tickets sul Server Centrale su Linux (moduli Centroen Open Ticket). Questo problema riguarda Centreon Open Tickets sul Server Centrale: da tutte le versioni precedenti a 25.10.3, 24.10.8, 24.04.7.

Descrizione Originale (EN): Vulnerability in Centreon Centreon Open Tickets on Central Server on Linux (Centroen Open Ticket modules).This issue affects Centreon Open Tickets on Central Server: from all before 25.10.3, 24.10.8, 24.04.7.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo del server centrale di monitoraggio Centreon. Ciò potrebbe portare al furto di dati sensibili, alla manipolazione dei sistemi monitorati o alla completa interruzione dei servizi aziendali critici.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.03% (Percentile: 0.07) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolate il server centrale Centreon, in particolare i moduli Open Tickets, in una VLAN o sottorete dedicata e strettamente segmentata. Implementate regole firewall restrittive per limitare l'accesso in ingresso e in uscita solo alle porte e agli indirizzi IP strettamente necessari e autorizzati, riducendo così la superficie d'attacco in attesa di una patch.

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28363 - CVSS 9.9 (CRITICA)

In OpenClaw prima del 23/02/2026, la validazione di tools.exec.safeBins per sort poteva essere aggirata tramite abbreviazioni di opzioni lunghe GNU (come –compress-prog) in modalità allowlist, portando a percorsi di esecuzione senza approvazione che erano destinati a richiedere approvazione. Solo una stringa esatta come –compress-program veniva negata.

Descrizione Originale (EN): In OpenClaw before 2026.2.23, tools.exec.safeBins validation for sort could be bypassed via GNU long-option abbreviations (such as –compress-prog) in allowlist mode, leading to approval-free execution paths that were intended to require approval. Only an exact string such as –compress-program was denied.

Cosa può succedere?

Un attaccante potrebbe aggirare i controlli di sicurezza ed eseguire comandi non autorizzati sui sistemi OpenClaw. Ciò consentirebbe la completa compromissione del sistema, il furto di dati sensibili e l'interruzione dei servizi critici.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.09% (Percentile: 0.25) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare i sistemi OpenClaw in una rete segmentata o DMZ dedicata con regole firewall restrittive che limitino il traffico in uscita. Questo limiterà la capacità di un attaccante di raggiungere o influenzare altri sistemi critici all'interno dell'infrastruttura, anche in caso di esecuzione non autorizzata di comandi.

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

184: **Incomplete List of Disallowed Inputs**

Termini Alternativi: Blacklist / Black List, Blocklist / Block List, Denylist / Deny List

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27941 - CVSS 9.9 (CRITICA)

OpenLIT è una piattaforma open source per l'ingegneria AI. Prima della versione 1.37.1, diversi flussi di lavoro GitHub Actions nel repository GitHub di OpenLIT utilizzavano l'evento 'pull_request_target' durante il checkout e l'esecuzione di codice non affidabile proveniente da pull request forkate. Questi flussi di lavoro vengono eseguiti con il contesto di sicurezza del repository di base, includendo un 'GITHUB_TOKEN' con privilegi di scrittura e numerose secrets sensibili (chiavi API, token per database/archivi vettoriali e una chiave di account di servizio Google Cloud). La versione 1.37.1 contiene una correzione.

Descrizione Originale (EN): OpenLIT is an open source platform for AI engineering. Prior to version 1.37.1, several GitHub Actions workflows in OpenLIT's GitHub repository use the 'pull_request_target' event while checking out and executing untrusted code from forked pull requests. These workflows run with the security context of the base repository, including a write-privileged 'GITHUB_TOKEN' and numerous sensitive secrets (API keys, database/vector store tokens, and a Google Cloud service account key). Version 1.37.1 contains a fix.

Cosa può succedere?

Un attaccante potrebbe eseguire codice arbitrario nel contesto del repository, rubando chiavi API e token sensibili. Ciò consentirebbe l'accesso non autorizzato a sistemi connessi, furto di dati critici e potenziale compromissione dell'intera piattaforma o della catena di fornitura software.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.04% (Percentile: 0.13) Disponibili 4 valori storici
Pubblicata:	26/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per migliorare la sicurezza dell'infrastruttura, isolare i runner di GitHub Actions in segmenti di rete dedicati. Implementare rigorose politiche di firewall e filtraggio in uscita (egress filtering) per limitare la loro connettività solo alle risorse strettamente indispensabili, prevenendo così l'accesso non autorizzato ad altri sistemi interni in caso di esecuzione di codice malevolo.

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

829: **Inclusion of Functionality from Untrusted Control Sphere**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28268 - CVSS 9.8 (CRITICA)

Vikunja è una piattaforma di gestione delle attività open-source e self-hosted. Le versioni precedenti alla 2.1.0 presentano una vulnerabilità nella logica di business nel meccanismo di reset della password di vikunja/api che consente ai token di reset della password di essere riutilizzati indefinitamente. A causa di una mancata invalidazione dei token dopo l'uso e di un bug critico nella routine di pulizia dei token (cron job), i token di reset rimangono validi per sempre. Ciò permette a un attaccante che intercetta un singolo token di reset (tramite log, cronologia del browser o phishing) di eseguire un completo e persistente takeover dell'account in qualsiasi momento futuro, bypassando i controlli di autenticazione standard. La versione 2.1.0 include una patch per questa vulnerabilità.

Descrizione Originale (EN): Vikunja is an open-source self-hosted task management platform. Versions prior to 2.1.0 have a business logic vulnerability exists in the password reset mechanism of vikunja/api that allows password reset tokens to be reused indefinitely. Due to a failure to invalidate tokens upon use and a critical logic bug in the token cleanup cron job, reset tokens remain valid forever. This allows an attacker who intercepts a single reset token (via logs, browser history, or phishing) to perform a complete, persistent account takeover at any point in the future, bypassing standard authentication controls. Version 2.1.0 contains a patch for the issue.

Cosa può succedere?

Un attaccante potrebbe ottenere accesso illimitato agli account utente, inclusi quelli amministrativi, sfruttando i token di reset password riutilizzabili. Questo consentirebbe il furto di dati sensibili, la manipolazione delle attività aziendali e gravi interruzioni operative, con il rischio di compromettere l'intera piattaforma di gestione.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.03% (Percentile: 0.10) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Data l'assenza di una patch, implementare un monitoraggio avanzato sui log dell'applicazione Vikunja e dell'infrastruttura sottostante. Concentrarsi sulla rilevazione di richieste di reset password multiple per lo stesso utente in un breve periodo o da indirizzi IP sospetti, e configurare alert automatici per notificare immediatamente il team di sicurezza.

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

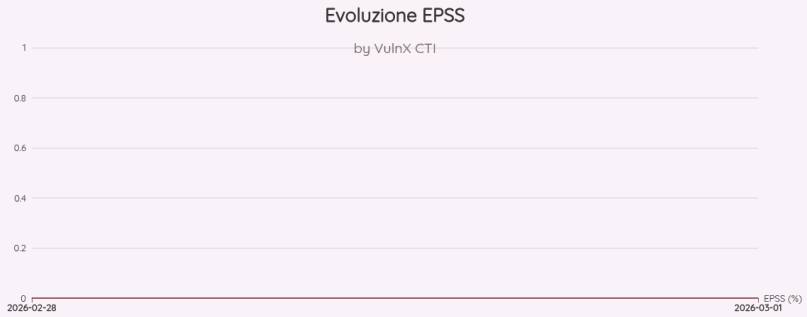
459: **Incomplete Cleanup**

Termini Alternativi: Insufficient Cleanup

640: **Weak Password Recovery Mechanism for Forgotten Password**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-28408 - CVSS 9.8 (CRITICA)

WeGIA è un gestore web per istituzioni benefiche. Prima della versione 3.6.5, lo script in adicionar_tipo_docs_atendido.php non passa attraverso il controller centrale del progetto e non dispone di controlli di autenticazione e autorizzazione propri. Un utente malintenzionato potrebbe effettuare una richiesta tramite strumenti come Postman o l'URL del file sul web per accedere a funzionalità riservate ai dipendenti. La vulnerabilità consente a soggetti esterni di iniettare dati non autorizzati in grandi quantità nel sistema di archiviazione del server dell'applicazione. La versione 3.6.5 risolve il problema.

Descrizione Originale (EN): WeGIA is a web manager for charitable institutions. Prior to version 3.6.5, the script in adicionar_tipo_docs_atendido.php does not go through the project's central controller and does not have its own authentication and permission checks. A malicious user could make a request through tools like Postman or the file's URL on the web to access features exclusive to employees. The vulnerability allows external parties to inject unauthorized data in massive quantities into the application server's storage. Version 3.6.5 fixes the issue.

Cosa può succedere?

Un aggressore esterno può accedere a funzionalità riservate ai dipendenti, consentendo l'iniezione di dati non autorizzati e la manipolazione di informazioni sensibili. Questo potrebbe portare a violazioni della privacy, danni alla reputazione e interruzioni operative per l'organizzazione.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.05% (Percentile: 0.16) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare una Web Application Firewall (WAF) o un reverse proxy davanti all'applicazione WeGIA. Configurare regole stringenti per bloccare l'accesso diretto allo script vulnerabile 'adicionar_tipo_docs_atendido.php' da fonti esterne non autorizzate, o limitarlo esclusivamente a indirizzi IP interni e fidati, agendo come controllo di accesso compensativo a livello di rete.

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

287: **Improper Authentication**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthC, AuthN, authentification

862: **Missing Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28411 - CVSS 9.8 (CRITICA)

WeGIA è un gestore web per istituzioni benefiche. Prima della versione 3.6.5, un uso insicuro della funzione 'extract()' sulla superglobale '$_REQUEST' consente a un attaccante non autenticato di sovrascrivere variabili locali in più script PHP. Questa vulnerabilità può essere sfruttata per bypassare completamente i controlli di autenticazione, consentendo l'accesso non autorizzato alle aree amministrative e protette dell'applicazione WeGIA. La versione 3.6.5 risolve il problema.

Descrizione Originale (EN): WeGIA is a web manager for charitable institutions. Prior to version 3.6.5, an unsafe use of the 'extract()' function on the '$_REQUEST' superglobal allows an unauthenticated attacker to overwrite local variables in multiple PHP scripts. This vulnerability can be leveraged to completely bypass authentication checks, allowing unauthorized access to administrative and protected areas of the WeGIA application. Version 3.6.5 fixes the issue.

Cosa può succedere?

Un attaccante non autenticato potrebbe ottenere pieno controllo dell'applicazione WeGIA, accedendo senza autorizzazione alle aree amministrative e protette. Questo consentirebbe il furto, la manipolazione o la distruzione di dati sensibili delle istituzioni benefiche, compromettendo gravemente la privacy e l'integrità delle operazioni.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.27% (Percentile: 0.50) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare questa vulnerabilità critica, implementare un Web Application Firewall (WAF) davanti all'applicazione WeGIA. Configurare il WAF per ispezionare e bloccare attivamente le richieste HTTP che tentano di manipolare parametri o iniettare variabili tramite la superglobale '$_REQUEST', prevenendo così i tentativi di bypass dell'autenticazione da parte di attaccanti non autenticati.

CVSS Metrics

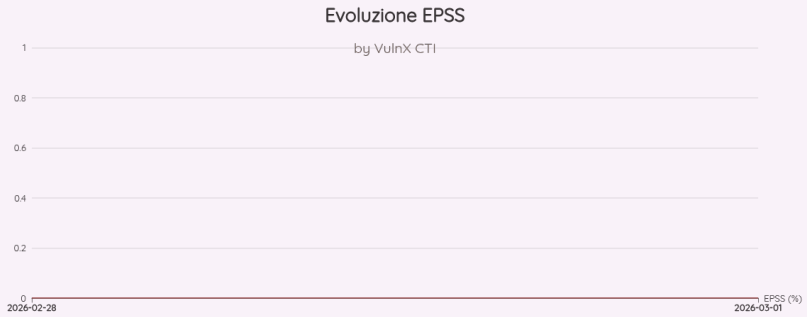
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

288: **Authentication Bypass Using an Alternate Path or Channel**

473: **PHP External Variable Modification**

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-27755 - CVSS 9.8 (CRITICA)

Le versioni del firmware SODOLA SL902-SWTGW124AS fino alla 200.1.20 presentano una vulnerabilità nella generazione dell'identificatore di sessione debole che consente agli attori malevoli di falsificare sessioni autenticate calcolando cookie prevedibili basati su MD5. Gli attaccanti che conoscono o indovinano credenziali valide possono calcolare offline l'identificatore di sessione e bypassare l'autenticazione senza completare il processo di login, ottenendo accesso non autorizzato al dispositivo.

Descrizione Originale (EN): SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 contain a weak session identifier generation vulnerability that allows attackers to forge authenticated sessions by computing predictable MD5-based cookies. Attackers who know or guess valid credentials can calculate the session identifier offline and bypass authentication without completing the login flow, gaining unauthorized access to the device.

Cosa può succedere?

Un malintenzionato potrebbe ottenere accesso non autorizzato ai dispositivi di rete, consentendo la compromissione del sistema. Ciò potrebbe causare gravi interruzioni dei servizi, reindirizzamento del traffico o furto di dati sensibili, oltre a fornire un punto d'appoggio per attacchi successivi alla rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.11% (Percentile: 0.29) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Per mitigare la vulnerabilità, implementare controlli di accesso rigorosi all'interfaccia di gestione dei dispositivi SODOLA SL902-SWTGW124AS. Limitare l'accesso a tale interfaccia esclusivamente a indirizzi IP predefiniti e autorizzati, idealmente da una rete di gestione segregata, per prevenire tentativi di calcolo offline e falsificazione delle sessioni.

CVSS Metrics

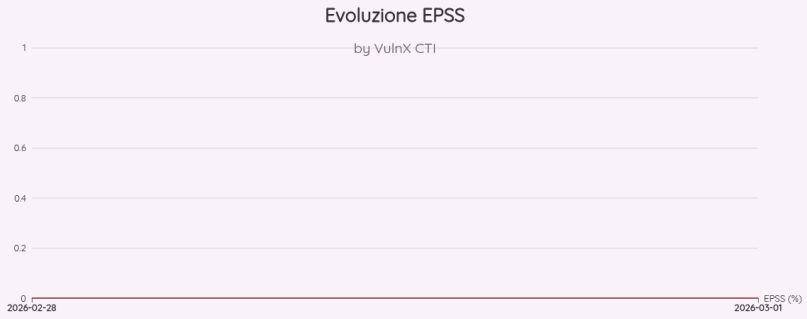
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

330: **Use of Insufficiently Random Values**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-2999 - CVSS 9.8 (CRITICA)

IDExpert Windows Logon Agent sviluppato da Changing presenta una vulnerabilità di Remote Code Execution, che consente agli attaccanti remoti non autenticati di forzare il sistema a scaricare file eseguibili arbitrari da una sorgente remota ed eseguirli.

Descrizione Originale (EN): IDExpert Windows Logon Agent developed by Changing has a Remote Code Execution vulnerability, allowing unauthenticated remote attackers to force the system to download arbitrary executable files from a remote source and execute them.

Cosa può succedere?

Un attaccante remoto non autenticato potrebbe ottenere il controllo completo del sistema, consentendo il furto di dati sensibili, l'interruzione dei servizi critici o l'installazione di malware come ransomware. Ciò potrebbe portare a una compromissione estesa dell'intera rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	02/03/2026
Modificata:	02/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolare i sistemi che eseguono IDExpert Windows Logon Agent in un segmento di rete dedicato o applicare regole firewall stringenti per limitare l'accesso al servizio esclusivamente da indirizzi IP interni e fidati. Questo riduce drasticamente la superficie di attacco per aggressori remoti non autenticati e impedisce loro di raggiungere la vulnerabilità.

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

494: **Download of Code Without Integrity Check**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-27751 - CVSS 9.8 (CRITICA)

Le versioni del firmware SODOLA SL902-SWTGW124AS fino alla 200.1.20 presentano una vulnerabilità legata alle credenziali di default che consente agli attaccanti remoti di ottenere l'accesso amministrativo all'interfaccia di gestione. Gli attaccanti possono autenticarsi utilizzando le credenziali di default hardcoded senza l'obbligo di modifica della password, ottenendo così il controllo amministrativo completo del dispositivo.

Descrizione Originale (EN): SODOLA SL902-SWTGW124AS firmware versions through 200.1.20 contain a default credentials vulnerability that allows remote attackers to obtain administrative access to the management interface. Attackers can authenticate using the hardcoded default credentials without password change enforcement to gain full administrative control of the device.

Cosa può succedere?

Un attaccante remoto potrebbe ottenere il controllo amministrativo completo del dispositivo, compromettendone le funzionalità. Questo permetterebbe interruzioni di servizio, il furto di dati sensibili e l'accesso non autorizzato ad altri sistemi della rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.13) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare l'interfaccia di gestione dei dispositivi SODOLA SL902-SWTGW124AS in un segmento di rete dedicato e altamente ristretto, non accessibile dalla rete principale o da Internet. Implementare controlli di accesso stringenti per assicurare che solo gli amministratori autorizzati, da host specifici e fidati o tramite connessioni VPN, possano raggiungere questa interfaccia.

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**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-3000 - CVSS 9.8 (CRITICA)

IDExpert Windows Logon Agent sviluppato da Changing presenta una vulnerabilità di Remote Code Execution, che consente agli attaccanti remoti non autenticati di forzare il sistema a scaricare file DLL arbitrari da una sorgente remota ed eseguirli.

Descrizione Originale (EN): IDExpert Windows Logon Agent developed by Changing has a Remote Code Execution vulnerability, allowing unauthenticated remote attackers to force the system to download arbitrary DLL files from a remote source and execute them.

Cosa può succedere?
Attaccanti remoti non autenticati possono ottenere il controllo completo dei sistemi aziendali. Questo permette il furto di dati sensibili, l'interruzione dei servizi critici e la potenziale compromissione dell'intera rete.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	02/03/2026
Modificata:	02/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare l'Application Whitelisting (es. Windows Defender Application Control o AppLocker) su tutti i sistemi che eseguono IDExpert Windows Logon Agent. Configurare queste policy per consentire l'esecuzione solo di applicazioni e DLL approvate, bloccando così l'esecuzione di file DLL arbitrari scaricati da sorgenti non autorizzate.

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

494: **Download of Code Without Integrity Check**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-3422 - CVSS 9.8 (CRITICA)

U-Office Force, sviluppato da e-Excellence, presenta una vulnerabilità di Insecure Deserialization, che consente a attori remoti non autenticati di eseguire codice arbitrario sul server inviando contenuti serializzati appositamente manipolati.

Descrizione Originale (EN): U-Office Force developed by e-Excellence has a Insecure Deserialization vulnerability, allowing unauthenticated remote attackers to execute arbitrary code on the server by sending maliciously crafted serialized content.

Cosa può succedere?

Un attaccante remoto può ottenere il pieno controllo del server, permettendo il furto di dati sensibili e l'interruzione dei servizi aziendali critici. Questo potrebbe anche portare alla diffusione dell'attacco ad altri sistemi interni, con gravi ripercussioni operative e finanziarie per l'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	02/03/2026
Modificata:	02/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolare immediatamente il server che ospita U-Office Force in una DMZ (Demilitarized Zone) o una rete segmentata dedicata. Configurare firewall per limitare rigorosamente l'accesso in ingresso a questo segmento, permettendo solo il traffico strettamente necessario da fonti fidate e bloccando ogni altro accesso diretto non autorizzato.

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, Unmarshaling, PHP Object Injection, Pickling, Unpickling

Approfondisci su VulnX

CVE-2026-24352 - CVSS 9.8 (CRITICA)

PluXml CMS consente di impostare l'identificatore di sessione di un utente prima dell'autenticazione. Il valore di questo ID di sessione rimane invariato dopo l'autenticazione. Questo comportamento permette a un attaccante di fissare un ID di sessione per una vittima e successivamente di hijackare la sessione autenticata. Il fornitore è stato avvisato tempestivamente di questa vulnerabilità, ma non ha risposto fornendo dettagli sulla vulnerabilità o sull'intervallo di versioni vulnerabili. Sono state testate e confermate vulnerabili solo le versioni 5.8.21 e 5.9.0-rc7; altre versioni non sono state testate e potrebbero essere anch'esse vulnerabili.

Descrizione Originale (EN): PluXml CMS allows a user's session identifier to be set before authentication. The value of this session ID stays the same after authentication. This behaviour enables an attacker to fix a session ID for a victim and later hijack the authenticated session. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only versions 5.8.21 and 5.9.0-rc7 were tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.

Cosa può succedere?

Un attaccante può dirottare le sessioni autenticate degli utenti del CMS, ottenendo accesso non autorizzato all'amministrazione. Questo può portare al furto di dati sensibili, alla manipolazione dei contenuti del sito web o alla compromissione completa del sistema, con gravi conseguenze per l'operatività e la reputazione aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.14) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare il rischio di session hijacking, implementare un Web Application Firewall (WAF) con regole specifiche. Configurare il WAF per rilevare e bloccare attivamente i tentativi di impostare o manipolare gli ID di sessione utente prima dell'autenticazione. Questo controllo compensativo ridurrà la superficie di attacco finché una patch non sarà disponibile.

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

384: **Session Fixation**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2025-11251 - CVSS 9.8 (CRITICA)

Vulnerabilità di Neutralizzazione Impropria di Elementi Speciali utilizzati in un Comando SQL ('SQL Injection') in Dayneks Software Industry and Trade Inc. E-Commerce Platform consente SQL Injection. Questo problema interessa E-Commerce Platform: attraverso 27022026. NOTA: Il fornitore è stato contattato tempestivamente riguardo a questa divulgazione, ma non ha risposto in alcun modo.

Descrizione Originale (EN): Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Dayneks Software Industry and Trade Inc. E-Commerce Platform allows SQL Injection.This issue affects E-Commerce Platform: through 27022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?
Sfruttare questa falla critica permetterebbe agli attaccanti di rubare dati sensibili dei clienti e informazioni aziendali riservate. Ciò potrebbe causare gravi perdite finanziarie, interruzioni del servizio e danni reputazionali significativi per l'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.01% (Percentile: 0.02) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un Web Application Firewall (WAF) davanti alla piattaforma e-commerce per filtrare il traffico e bloccare proattivamente i tentativi di SQL Injection. Configurare il WAF con regole specifiche per rilevare e neutralizzare input malevoli, fungendo da controllo compensativo essenziale per proteggere l'applicazione vulnerabile a livello infrastrutturale in assenza di una patch.

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

89: **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: SQL injection, SQLi

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2025-11252 - CVSS 9.8 (CRITICA)

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Signum Technology Promotion and Training Inc. Windesk.Fm consente l'SQL Injection. Questo problema interessa windesk.Fm: fino al 27022026. NOTA: Il fornitore è stato contattato tempestivamente riguardo a questa divulgazione, ma non ha risposto in alcun modo.

Descrizione Originale (EN): Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Signum Technology Promotion and Training Inc. Windesk.Fm allows SQL Injection.This issue affects windesk.Fm: through 27022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?

Sfruttare questa vulnerabilità critica permette agli attaccanti di accedere, modificare o cancellare dati sensibili aziendali, come informazioni clienti e finanziarie, causando gravi violazioni dei dati. Inoltre, potrebbe portare alla compromissione totale del sistema, con conseguenti interruzioni dei servizi, perdite economiche e danni reputazionali significativi.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.03% (Percentile: 0.09) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	28/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare urgentemente un Web Application Firewall (WAF) a protezione dell'applicazione Windesk.Fm. Configurare il WAF per ispezionare e filtrare il traffico HTTP/S in ingresso, bloccando proattivamente i tentativi di SQL Injection prima che raggiungano l'applicazione vulnerabile. Questa misura di controllo compensativo è cruciale per mitigare la grave vulnerabilità in assenza di una patch.

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

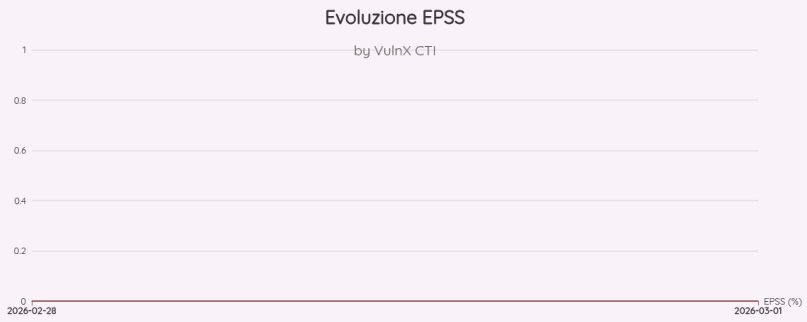
CWE - Common Weakness Enumeration

89: **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: SQL injection, SQLi

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2025-12981 - CVSS 9.8 (CRITICA)

Il tema Listee per WordPress è vulnerabile a escalation dei privilegi in tutte le versioni fino, e inclusa, 1.1.6. Ciò è dovuto a un controllo di convalida difettoso nella funzione di registrazione utente del plugin listee-core integrato, che non sanifica correttamente il parametro user_role. Questo rende possibile agli attaccanti non autenticati registrarsi come Administrator manipolando il parametro user_role durante la registrazione.

Descrizione Originale (EN): The Listee theme for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.1.6. This is due to a broken validation check in the bundled listee-core plugin's user registration function that fails to properly sanitize the user_role parameter. This makes it possible for unauthenticated attackers to register as Administrator by manipulating the user_role parameter during registration.

Cosa può succedere?

Un attaccante può ottenere il controllo amministrativo completo del sito web aziendale. Questo permette il furto di dati sensibili, la manipolazione dei contenuti o l'interruzione dei servizi, causando gravi danni alla reputazione e perdite finanziarie per l'organizzazione.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare una regola su un Web Application Firewall (WAF) per bloccare o ispezionare le richieste di registrazione utente che tentano di manipolare il parametro 'user_role' e assegnare ruoli privilegiati come 'administrator'. Questo controllo compensativo a livello di infrastruttura previene efficacemente l'escalation di privilegi da parte di attaccanti non autenticati, mitigando la vulnerabilità in assenza di una patch.

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-2251 - CVSS 9.8 (CRITICA)

Vulnerabilità di limitazione impropria di un pathname a una directory ristretta (Path Traversal) in Xerox FreeFlow Core consente un attraversamento non autorizzato del percorso che può portare a RCE. Questo problema riguarda le versioni di Xerox FreeFlow Core fino alla 8.0.7 inclusa. Si consiglia di aggiornare a FreeFlow Core versione 8.1.0 tramite il software disponibile su - https://www.support.xerox.com/en-us/product/core/downloads https://www.support.xerox.com/en-us/product/core/downloads

Descrizione Originale (EN): Improper limitation of a pathname to a restricted directory (Path Traversal) vulnerability in Xerox FreeFlow Core allows unauthorized path traversal leading to RCE. This issue affects Xerox FreeFlow Core versions up to and including 8.0.7. Please consider upgrading to FreeFlow Core version 8.1.0 via the software available on - https://www.support.xerox.com/en-us/product/core/downloads https://www.support.xerox.com/en-us/product/core/downloads

Cosa può succedere?
Sfruttando questa vulnerabilità, un attaccante potrebbe ottenere il controllo completo dei sistemi Xerox FreeFlow Core. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi critici o all'installazione di software malevolo, causando gravi danni operativi e reputazionali all'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.05% (Percentile: 0.17) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolare il server Xerox FreeFlow Core in un segmento di rete dedicato (VLAN/subnet) con regole firewall restrittive. Implementare un filtraggio rigoroso del traffico in ingresso e in uscita, consentendo solo le comunicazioni essenziali per il suo funzionamento e limitando la superficie di attacco in caso di compromissione.

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

22: **Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')**

Probabilità di Sfruttamento: high

Termini Alternativi: Directory traversal, Path traversal

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-3301 - CVSS 9.8 (CRITICA)

È stata scoperta una vulnerabilità di sicurezza in Totolink N300RH 6.1c.1353_B20190305. A rischio è la funzione setWebWlanIdx del file /cgi-bin/cstecgi.cgi del componente Web Management Interface. La manipolazione dell'argomento webWlanIdx può portare a un'iniezione di comandi OS. L'attacco può essere eseguito da remoto. L'exploit è stato reso pubblico e potrebbe essere utilizzato per attacchi.

Descrizione Originale (EN): A security flaw has been discovered in Totolink N300RH 6.1c.1353_B20190305. Affected by this vulnerability is the function setWebWlanIdx of the file /cgi-bin/cstecgi.cgi of the component Web Management Interface. Performing a manipulation of the argument webWlanIdx results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo del dispositivo di rete, compromettendo l'intera infrastruttura aziendale. Ciò potrebbe causare il furto di dati sensibili, l'interruzione prolungata dei servizi critici e la compromissione di altri sistemi interni.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	2.90% (Percentile: 0.86) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare il dispositivo Totolink N300RH in una rete di gestione dedicata (VLAN) e implementare rigorosi controlli di accesso tramite firewall. Consentire l'accesso all'interfaccia web di gestione solo da indirizzi IP specifici e autorizzati all'interno della rete interna, bloccando ogni tentativo di connessione da reti non attendibili o da Internet.

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

77: **Improper Neutralization of Special Elements used in a Command ('Command Injection')**

Probabilità di Sfruttamento: high

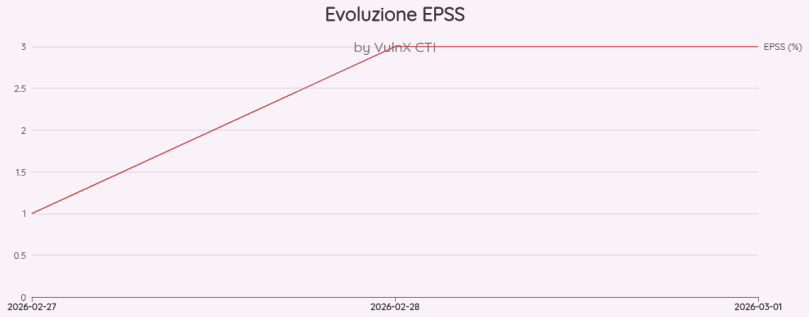
Termini Alternativi: Command injection

78: **Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: OS Command Injection, Shell injection, Shell metacharacters

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-28213 - CVSS 9.8 (CRITICA)

EverShop è una piattaforma eCommerce basata principalmente su TypeScript. Le versioni precedenti alla 2.1.1 presentano una vulnerabilità nella funzionalità "Password Dimenticata". Quando si specifica un indirizzo email di destinazione, la risposta dell'API restituisce il password reset token. Ciò consente a un attaccante di prendere il controllo dell'account associato. La versione 2.1.1 risolve il problema.

Descrizione Originale (EN): EverShop is a TypeScript-first eCommerce platform. Versions prior to 2.1.1 have a vulnerability in the 'Forgot Password' functionality. When specifying a target email address, the API response returns the password reset token. This allows an attacker to take over the associated account. Version 2.1.1 fixes the issue.

Cosa può succedere?

Un attaccante può prendere il controllo degli account utente su piattaforme EverShop, accedendo a dati sensibili dei clienti e potendo effettuare acquisti fraudolenti. Questo può comportare significative perdite finanziarie per l'azienda, danni alla reputazione e violazioni della privacy dei dati dei clienti.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.13) Disponibili 3 valori storici
Pubblicata:	26/02/2026
Modificata:	28/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) per monitorare e filtrare il traffico verso l'API di reset della password della piattaforma EverShop. Configurare il WAF per rilevare e bloccare tentativi anomali di richiesta di token o per ispezionare le risposte dell'API, impedendo la fuoriuscita del token di reset.

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

200: **Exposure of Sensitive Information to an Unauthorized Actor**

Probabilità di Sfruttamento: high

Termini Alternativi: Information Disclosure, Information Leak

---

640: **Weak Password Recovery Mechanism for Forgotten Password**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-22207 - CVSS 9.8 (CRITICA)

OpenViking fino alla versione 0.1.18, prima del commit 0251c70, presenta una vulnerabilità di broken access control che consente agli attaccanti non autenticati di ottenere privilegi ROOT quando la configurazione root_api_key viene omessa. Gli attaccanti possono inviare richieste agli endpoint protetti senza intestazioni di autenticazione per accedere a funzioni amministrative tra cui gestione degli account, operazioni sulle risorse e configurazione del sistema.

Descrizione Originale (EN): OpenViking through version 0.1.18, prior to commit 0251c70, contains a broken access control vulnerability that allows unauthenticated attackers to gain ROOT privileges when the root_api_key configuration is omitted. Attackers can send requests to protected endpoints without authentication headers to access administrative functions including account management, resource operations, and system configuration.

Cosa può succedere?

Un attaccante non autenticato può ottenere il controllo ROOT del sistema, consentendo il furto di dati sensibili, la manipolazione delle configurazioni critiche e l'interruzione dei servizi. Questo comporta gravi rischi di perdita finanziaria e danni alla reputazione aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.17% (Percentile: 0.39) Disponibili 3 valori storici
Pubblicata:	26/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementate un Web Application Firewall (WAF) o un API Gateway davanti all'istanza di OpenViking. Configuratelo per bloccare o richiedere un'autenticazione esplicita per tutte le richieste dirette agli endpoint amministrativi, soprattutto se prive dell'intestazione 'root_api_key', mitigando l'accesso non autorizzato.

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2025-50857 - CVSS 9.8 (CRITICA)

ZenTaoPMS dalla versione 18.11 alla versione 21.6.beta è vulnerabile a Directory Traversal in /module/ai/control.php. Ciò consente agli attaccanti di eseguire codice arbitrario tramite un caricamento di file manipolato

Descrizione Originale (EN): ZenTaoPMS v18.11 through v21.6.beta is vulnerable to Directory Traversal in /module/ai/control.php. This allows attackers to execute arbitrary code via a crafted file upload

Cosa può succedere?

Gli attaccanti potrebbero ottenere il controllo completo del server che esegue ZenTaoPMS. Ciò consentirebbe il furto di dati sensibili, l'interruzione dei servizi critici e la possibilità di compromettere ulteriormente altri sistemi aziendali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.58% (Percentile: 0.68) Disponibili 3 valori storici
Pubblicata:	26/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) per monitorare e bloccare tentativi di upload di file manipolati o attacchi di Directory Traversal verso l'applicazione ZenTaoPMS. Configurare inoltre permessi restrittivi sul filesystem per le directory di upload, negando l'esecuzione di script e consentendo la scrittura solo quando strettamente indispensabile, per mitigare l'esecuzione di codice arbitrario.

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

22: **Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')**

Probabilità di Sfruttamento: high

Termini Alternativi: Directory traversal, Path traversal

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27966 - CVSS 9.8 (CRITICA)

Langflow è uno strumento per la creazione e il deployment di agent e workflow alimentati da AI. Prima della versione 1.8.0, il nodo CSV Agent in Langflow aveva hardcoded 'allow_dangerous_code=True', il che esponeva automaticamente lo strumento Python REPL di LangChain ('python_repl_ast'). Di conseguenza, un attaccante può eseguire comandi Python e OS arbitrari sul server tramite prompt injection, portando a una piena Remote Code Execution (RCE). La versione 1.8.0 risolve il problema.

Descrizione Originale (EN): Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.8.0, the CSV Agent node in Langflow hardcodes 'allow_dangerous_code=True', which automatically exposes LangChain's Python REPL tool ('python_repl_ast'). As a result, an attacker can execute arbitrary Python and OS commands on the server via prompt injection, leading to full Remote Code Execution (RCE). Version 1.8.0 fixes the issue.

Cosa può succedere?

Un attaccante può ottenere il controllo completo del server che esegue Langflow. Questo permetterebbe il furto di dati sensibili, l'interruzione dei servizi aziendali critici o l'installazione di software dannoso per compromettere ulteriormente l'ambiente.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.31% (Percentile: 0.54) Disponibili 4 valori storici
Pubblicata:	26/02/2026
Modificata:	28/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolate il server Langflow in un segmento di rete dedicato e strettamente controllato, come una DMZ o una VLAN separata. Implementate regole firewall restrittive per limitare le connessioni in ingresso e in uscita solo a quelle strettamente necessarie, riducendo significativamente il raggio d'azione di un potenziale attaccante in caso di compromissione.

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

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25952 - CVSS 9.8 (CRITICA)

FreeRDP è una implementazione gratuita del Remote Desktop Protocol. Prima della versione 3.23.0, ‘xf_SetWindowMinMaxInfo‘ dereferenziava un puntatore ‘xfAppWindow‘ già liberato perché ‘xf_rail_get_window‘ in ‘xf_rail_server_min_max_info‘ restituisce un puntatore non protetto dalla tabella hash ‘railWindows‘, e il thread principale può eliminare contemporaneamente la finestra (tramite un ordine di eliminazione finestra) mentre il thread del canale RAIL sta ancora utilizzando il puntatore. La versione 3.23.0 risolve il problema.

Descrizione Originale (EN): FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, ‘xf_SetWindowMinMaxInfo‘ dereferences a freed ‘xfAppWindow‘ pointer because ‘xf_rail_get_window‘ in ‘xf_rail_server_min_max_info‘ returns an unprotected pointer from the ‘railWindows‘ hash table, and the main thread can concurrently delete the window (via a window delete order) while the RAIL channel thread is still using the pointer. Version 3.23.0 fixes the issue.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo dei sistemi che utilizzano FreeRDP vulnerabile. Ciò potrebbe portare al furto di dati sensibili, all’interruzione dei servizi critici e alla possibilità di estendere l’attacco ad altri sistemi della rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.07% (Percentile: 0.21) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolate i sistemi che utilizzano FreeRDP su un segmento di rete dedicato, accessibile esclusivamente tramite jump box sicuri o un gateway protetto (es. VPN/bastion host), e non direttamente esposti a reti non fidate. Questo riduce drasticamente la superficie di attacco e la probabilità di sfruttamento della vulnerabilità.

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

416: **Use After Free**

Probabilità di Sfruttamento: high

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25953 - CVSS 9.8 (CRITICA)

FreeRDP è una implementazione gratuita del Remote Desktop Protocol. Prima della versione 3.23.0, ‘xf_AppUpdateWindowFromSurface‘ leggeva da un ‘xfAppWindow‘ già liberato perché il thread RDPGFX DVC ottiene un puntatore nudo tramite ‘xf_rail_get_window‘ senza alcuna protezione di durata, mentre il thread principale può eliminare contemporaneamente la finestra tramite un ordine di eliminazione finestra fastpath. La versione 3.23.0 risolve il problema.

Descrizione Originale (EN): FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, ‘xf_AppUpdateWindowFromSurface‘ reads from a freed ‘xfAppWindow‘ because the RDPGFX DVC thread obtains a bare pointer via ‘xf_rail_get_window‘ without any lifetime protection, while the main thread can concurrently delete the window through a fastpath window-delete order. Version 3.23.0 fixes the issue.

Cosa può succedere?

Un aggressore potrebbe ottenere il controllo completo dei sistemi esposti, rubare dati sensibili e causare interruzioni significative ai servizi aziendali. Questo comporta un rischio elevato di compromissione dell’infrastruttura e gravi perdite operative o finanziarie.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.07% (Percentile: 0.21) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Data l’assenza di una patch e la gravità critica della vulnerabilità, si raccomanda di disabilitare l’uso di FreeRDP sui sistemi critici o di adottare soluzioni alternative per l’accesso remoto. Se la disabilitazione non è fattibile, isolare i client FreeRDP in un segmento di rete dedicato, implementando rigide regole firewall che consentano connessioni RDP solo verso destinazioni fidate e strettamente necessarie.

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

416: **Use After Free**

Probabilità di Sfruttamento: high

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25955 - CVSS 9.8 (CRITICA)

FreeRDP è un'implementazione gratuita del Remote Desktop Protocol. Prima della versione 3.23.0, 'xf_AppUpdateWindowFromSurface' riutilizzava un 'XImage' cacheato il cui puntatore 'data' fa riferimento a un buffer di superficie RDPGFX liberato, poiché 'gdi_DeleteSurface' libera 'surface->data' senza invalidare 'appWindow->image' che lo aliasa. La versione 3.23.0 risolve il problema.

Descrizione Originale (EN): FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, 'xf_AppUpdateWindowFromSurface' reuses a cached 'XImage' whose 'data' pointer references a freed RDPGFX surface buffer, because 'gdi_DeleteSurface' frees 'surface->data' without invalidating the 'appWindow->image' that aliases it. Version 3.23.0 fixes the issue.

Cosa può succedere?

Un aggressore remoto potrebbe ottenere il controllo completo dei sistemi che utilizzano FreeRDP. Questo permetterebbe il furto di dati sensibili, la manipolazione di informazioni critiche e l'interruzione dei servizi aziendali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.05% (Percentile: 0.16) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

In attesa di una patch, implementare una stretta segmentazione di rete e controlli d'accesso per i sistemi che utilizzano FreeRDP. Configurare i firewall per consentire le connessioni RDP in uscita dai client FreeRDP esclusivamente verso server RDP interni e di fiducia. Bloccare ogni altra destinazione per prevenire connessioni a server RDP malevoli che

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

416: **Use After Free**

Probabilità di Sfruttamento: high

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25959 - CVSS 9.8 (CRITICA)

FreeRDP è una implementazione gratuita del Remote Desktop Protocol. Prima della versione 3.23.0, ‘xf_cliprdr_provide_data_‘ passava ‘pDstData‘ liberato a ‘XChangeProperty‘ perché il thread del canale cliprdr chiamava ‘xf_cliprdr_server_format_data_response‘, che converteva e utilizzava i dati degli appunti senza mantenere alcun lock, mentre il thread degli eventi X11 chiamava contemporaneamente ‘xf_cliprdr_clear_cached_data‘ □ ‘HashTable_Clear‘, che liberava gli stessi dati tramite ‘xf_cached_data_free‘, causando un uso di heap dopo averli liberati. La versione 3.23.0 risolve il problema.

Descrizione Originale (EN): FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, ‘xf_cliprdr_provide_data_‘ passes freed ‘pDstData‘ to ‘XChangeProperty‘ because the cliprdr channel thread calls ‘xf_cliprdr_server_format_data_response‘ which converts and uses the clipboard data without holding any lock, while the X11 event thread concurrently calls ‘xf_cliprdr_clear_cached_data‘ □ ‘HashTable_Clear‘ which frees the same data via ‘xf_cached_data_free‘, triggering a heap use after free. Version 3.23.0 fixes the issue.

Cosa può succedere?

Sfruttando questa vulnerabilità critica, un attaccante potrebbe ottenere il controllo completo dei sistemi remoti. Ciò potrebbe portare al furto di dati sensibili, alla compromissione dell’integrità dei sistemi e a gravi interruzioni dei servizi aziendali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.06% (Percentile: 0.20) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Considerando che la vulnerabilità è legata alla gestione del reindirizzamento degli appunti (clipboard redirection) in FreeRDP, disabilitare questa funzionalità sui server interessati come misura di controllo compensativo. Questo ridurrà significativamente la superficie di attacco e il rischio di sfruttamento fino alla disponibilità di una patch.

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

416: **Use After Free**

Probabilità di Sfruttamento: high

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25997 - CVSS 9.8 (CRITICA)

FreeRDP è un'implementazione gratuita del Remote Desktop Protocol. Prima della versione 3.23.0, 'xf_clipboard_format_equal' leggeva memoria già liberata di 'lastSentFormats' perché 'xf_clipboard_formats_free' (chiamata dal thread del canale cliprdr durante il riconnessione automatica) libera l'array mentre il thread degli eventi X11 lo itera contemporaneamente in 'xf_clipboard_changed', causando un uso dopo free dell'heap. La versione 3.23.0 risolve il problema.

Descrizione Originale (EN): FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.23.0, 'xf_clipboard_format_equal' reads freed 'lastSentFormats' memory because 'xf_clipboard_formats_free' (called from the cliprdr channel thread during auto-reconnect) frees the array while the X11 event thread concurrently iterates it in 'xf_clipboard_changed', triggering a heap use after free. Version 3.23.0 fixes the issue.

Cosa può succedere?

Un attaccante potrebbe eseguire codice malevolo sul sistema che utilizza FreeRDP, ottenendo il controllo completo. Ciò potrebbe portare al furto di dati sensibili, alla compromissione totale del sistema o all'interruzione dei servizi critici.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.07% (Percentile: 0.21) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare una rigorosa segmentazione di rete per isolare i sistemi client che utilizzano FreeRDP. Restringere le connessioni RDP in uscita da tali client solo a server RDP fidati e strettamente necessari, utilizzando firewall per bloccare tutti gli altri tentativi di connessione.

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

416: **Use After Free**

Probabilità di Sfruttamento: high

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27510 - CVSS 9.6 (CRITICA)

Le versioni del firmware Unitree Go2 dalla 1.1.7 alla 1.1.11, utilizzate con l'applicazione Android Unitree Go2 (com.unitree.doggo2), sono vulnerabili a esecuzione remota di codice a causa della mancanza di protezione dell'integrità e della validazione dei programmi creati dall'utente. L'applicazione Android memorizza i programmi in un database SQLite locale (unitree_go2.db, tabella dog_programme) e trasmette il contenuto di programme_text, inclusa la field pyCode, al robot. L'actuator_manager.py del robot esegue il Python fornito come root senza verifiche di integrità o validazione del contenuto. Un attaccante con accesso locale al dispositivo Android può alterare il record del programma memorizzato per iniettare Python arbitrario che viene eseguito quando l'utente attiva il programma tramite un keybinding del controller, e il binding dannoso persiste anche dopo il riavvio. Inoltre, un programma dannoso condiviso tramite il marketplace della community dell'applicazione può portare all'esecuzione di codice arbitrario su qualsiasi robot che lo importi e lo esegua.

Descrizione Originale (EN): Unitree Go2 firmware versions 1.1.7 through 1.1.11, when used with the Unitree Go2 Android application (com.unitree.doggo2), are vulnerable to remote code execution due to missing integrity protection and validation of user-created programmes. The Android application stores programs in a local SQLite database (unitree_go2.db, table dog_programme) and transmits the programme_text content, including the pyCode field, to the robot. The robot's actuator_manager.py executes the supplied Python as root without integrity verification or content validation. An attacker with local access to the Android device can tamper with the stored programme record to inject arbitrary Python that executes when the user triggers the program via a controller keybinding, and the malicious binding persists across reboots. Additionally, a malicious program shared through the application's community marketplace can result in arbitrary code execution on any robot that imports and runs it.

Cosa può succedere?

Un attaccante potrebbe prendere il controllo completo dei robot Unitree Go2, manipolandone le operazioni o disabilitandoli. Questo potrebbe causare gravi interruzioni dei servizi aziendali, danni fisici alle apparecchiature o all'ambiente, e compromettere la sicurezza operativa.

Punteggio CVSS:	9.6 (CRITICA)
EPSS:	0.08% (Percentile: 0.23) Disponibili 3 valori storici
Pubblicata:	26/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare una segmentazione di rete rigorosa, isolando i robot Unitree Go2 e i relativi dispositivi di controllo Android su una VLAN dedicata e con accesso strettamente limitato. Questo impedirà che un'eventuale compromissione dei robot, tramite l'esecuzione di codice remoto, si propaghi ad altri segmenti di rete critici.

CVSS Metrics

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

CWE - Common Weakness Enumeration

345: **Insufficient Verification of Data Authenticity**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27493 - CVSS 9.5 (CRITICA)

n8n è una piattaforma open source di automazione dei workflow. Prima delle versioni 2.10.1, 2.9.3 e 1.123.22, esisteva una vulnerabilità di injection di espressioni di secondo ordine nei nodi Form di n8n che poteva consentire a un attaccante non autenticato di iniettare e valutare arbitrariamente espressioni n8n inviando dati di modulo appositamente manipolati. Quando combinata con un escape del sandbox di espressione, questa vulnerabilità poteva portare a un'esecuzione remota di codice sull'host n8n. La vulnerabilità richiede una configurazione specifica del workflow per essere sfruttata. Innanzitutto, un nodo form con un campo che interpola un valore fornito da un utente non autenticato, ad esempio un valore inviato tramite modulo. In secondo luogo, il valore del campo deve iniziare con un carattere '=', che induce n8n a trattarlo come un'espressione e attiva una doppia valutazione del contenuto del campo. Non vi è alcun motivo pratico per un progettista di workflow di anteporre intenzionalmente un '=' a un campo — il carattere non viene renderizzato nell'output, quindi il risultato non corrisponderebbe alle aspettative del progettista. Se aggiunto accidentalmente, sarebbe facilmente riconoscibile e molto improbabile che persista. Un attaccante non autenticato dovrebbe conoscere questa circostanza specifica su un'istanza target o scoprire casualmente un modulo corrispondente. Anche quando i prerequisiti sono soddisfatti, l'injection di espressioni da sola è limitata ai dati accessibili all'interno del contesto delle espressioni di n8n. L'escalation a esecuzione remota di codice richiede il chaining con una vulnerabilità separata di escape del sandbox. Il problema è stato risolto nelle versioni 2.10.1, 2.9.3 e 1.123.22 di n8n. Gli utenti dovrebbero aggiornare a una di queste versioni o successive per mitigare la vulnerabilità. Se l'aggiornamento non è immediatamente possibile, gli amministratori dovrebbero considerare le seguenti mitigazioni temporanee. Revisionare manualmente l'uso dei nodi form per verificare le condizioni sopra menzionate, disabilitare il nodo Form aggiungendo 'n8n-nodes-base.form' alla variabile di ambiente 'NODES_EXCLUDE', e/o disabilitare il nodo Form Trigger aggiungendo 'n8n-nodes-base.formTrigger' alla variabile di ambiente 'NODES_EXCLUDE'. Queste soluzioni temporanee non eliminano completamente il rischio e dovrebbero essere utilizzate solo come misure di mitigazione a breve termine.

Descrizione Originale (EN): n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, a second-order expression injection vulnerability existed in n8n's Form nodes that could allow an unauthenticated attacker to inject and evaluate arbitrary n8n expressions by submitting crafted form data. When chained with an expression sandbox escape, this could escalate to remote code execution on the n8n host. The vulnerability requires a specific workflow configuration to be exploitable. First, a form node with a field interpolating a value provided by an unauthenticated user, e.g. a form submitted value. Second, the field value must begin with an '=' character, which caused n8n to treat it as an expression and triggered a double-evaluation of the field content. There is no practical reason for a workflow designer to prefix a field with '=' intentionally — the character is not rendered in the output, so the result would not match the designer's expectations. If added accidentally, it would be noticeable and very unlikely to persist. An unauthenticated attacker would need to either know about this specific circumstance on a target instance or discover a matching form by chance. Even when the preconditions are met, the expression injection alone is limited to data accessible within the n8n expression context. Escalation to remote code execution requires chaining with a separate sandbox escape vulnerability. The issue has been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22.

Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Review usage of form nodes manually for above mentioned preconditions, disable the Form node by adding 'n8n-nodes-base.form' to the 'NODES_EXCLUDE' environment variable, and/or disable the Form Trigger node by adding 'n8n-nodes-base.formTrigger' to the 'NODES_EXCLUDE' environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.

Cosa può succedere?
Un aggressore non autenticato potrebbe ottenere il controllo completo del sistema n8n, portando al furto di dati sensibili. Ciò potrebbe causare gravi interruzioni dei servizi e compromettere l'integrità dell'intera infrastruttura aziendale.

Punteggio CVSS:	9.5 (CRITICA)
EPSS:	0.14% (Percentile: 0.35) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolare l'istanza di n8n in un segmento di rete dedicato, limitando l'accesso diretto da internet pubblico. Implementare un Web Application Firewall (WAF) davanti all'applicazione n8n per filtrare e bloccare i dati di modulo appositamente manipolati e i tentativi di injection, riducendo il rischio di valutazione non autenticata di espressioni.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

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

Probabilità di Sfruttamento: medium

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27947 - CVSS 9.4 (CRITICA)

Group-Office è uno strumento di gestione delle relazioni con i clienti e groupware per aziende. Le versioni precedenti alla 26.0.9, 25.0.87 e 6.8.154 presentano una vulnerabilità di Remote Code Execution autenticata nel flusso di elaborazione degli allegati TNEF. Il percorso vulnerabile estrae file controllati dall'attaccante da 'winmail.dat' e successivamente invoca 'zip' con un carattere jolly di shell ('*'). Poiché i nomi dei file estratti sono controllati dall'attaccante, possono essere interpretati come opzioni di 'zip' e portare all'esecuzione arbitraria di comandi. Le versioni 26.0.9, 25.0.87 e 6.8.154 risolvono il problema.

Descrizione Originale (EN): Group-Office is an enterprise customer relationship management and groupware tool. Versions prior to 26.0.9, 25.0.87, and 6.8.154 have an authenticated Remote Code Execution vulnerability in the TNEF attachment processing flow. The vulnerable path extracts attacker-controlled files from 'winmail.dat' and then invokes 'zip' with a shell wildcard ('*'). Because extracted filenames are attacker-controlled, they can be interpreted as 'zip' options and lead to arbitrary command execution. Versions 26.0.9, 25.0.87, and 6.8.154 fix the issue.

Cosa può succedere?

Un attaccante autenticato può eseguire codice malevolo sul server Group-Office. Questo permetterebbe il furto di dati aziendali sensibili, la compromissione totale del sistema e la potenziale interruzione dei servizi essenziali.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.30% (Percentile: 0.53) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Eseguire il servizio Group-Office con un account utente con i privilegi minimi indispensabili e implementare una soluzione di whitelisting delle applicazioni sul server. Questo impedirà l'esecuzione di binari non autorizzati e limiterà drasticamente l'impatto di un'eventuale esecuzione di codice remoto da parte di un attaccante.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** low
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

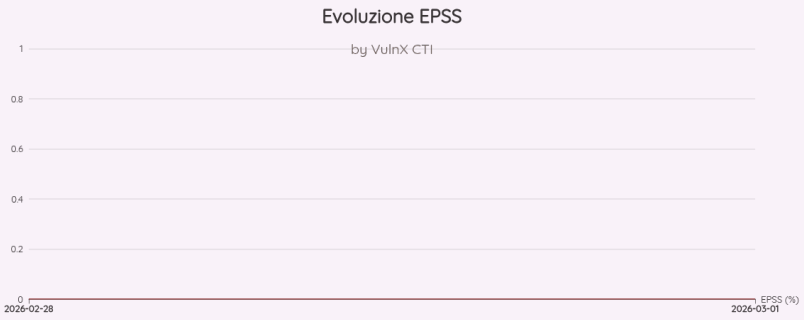
88: **Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')**

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Unrestricted File Upload

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-25851 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazione non autorizzata delle stazioni e manipolare i dati inviati al backend. Un attaccante non autenticato può connettersi all'endpoint WebSocket OCPP utilizzando un identificatore di stazione di ricarica noto o scoperto, quindi inviare o ricevere comandi OCPP come un caricatore legittimo. Dato che non è richiesta alcuna autenticazione, ciò può portare a escalation dei privilegi, controllo non autorizzato dell'infrastruttura di ricarica e corruzione dei dati della rete di ricarica riportati al backend.

Descrizione Originale (EN): WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.

Cosa può succedere?
Sfruttando questa falla, è possibile impersonare le stazioni di ricarica e manipolare i dati inviati al backend. Ciò può causare interruzioni del servizio, dati di fatturazione errati e significativi danni operativi o finanziari per l'azienda.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.13% (Percentile: 0.33) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un gateway API o un reverse proxy in fronte agli endpoint WebSocket OCPP. Configurare questo componente per imporre un'autenticazione robusta e controlli di autorizzazione (es. mTLS o autenticazione basata su token) per tutte le connessioni in ingresso. Questo agirà da strato di sicurezza compensativo, garantendo che solo le entità autorizzate possano interagire con il servizio, mitigando il rischio di impersonificazione.

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:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-24731 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazione non autorizzata delle stazioni e manipolare i dati inviati al backend. Un attaccante non autenticato può connettersi all'endpoint WebSocket OCPP utilizzando un identificatore di stazione di ricarica noto o scoperto, quindi inviare o ricevere comandi OCPP come un caricatore legittimo. Dato che non è richiesta alcuna autenticazione, ciò può portare a escalation dei privilegi, controllo non autorizzato dell'infrastruttura di ricarica e corruzione dei dati della rete di ricarica riportati al backend.

Descrizione Originale (EN): WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.

Cosa può succedere?

Un attaccante può impersonare stazioni di ricarica legittime, manipolare i dati di sistema e controllare le operazioni. Ciò può causare gravi interruzioni del servizio, transazioni non autorizzate e significative perdite finanziarie e di reputazione per l'azienda.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.13% (Percentile: 0.33) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare la vulnerabilità, implementare un reverse proxy o un API Gateway davanti all'endpoint WebSocket OCPP. Questo componente esterno deve imporre meccanismi di autenticazione e autorizzazione robusti, garantendo che solo le stazioni di ricarica autenticate possano stabilire connessioni e inviare comandi. Tale controllo compensativo blocca l'accesso non autorizzato a livello di infrastruttura, indipendentemente dalla logica applicativa.

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:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-20781 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazione non autorizzata delle stazioni e manipolare i dati inviati al backend. Un attaccante non autenticato può connettersi all'endpoint WebSocket OCPP utilizzando un identificatore di stazione di ricarica noto o scoperto, quindi inviare o ricevere comandi OCPP come un caricatore legittimo. Dato che non è richiesta alcuna autenticazione, ciò può portare a escalation dei privilegi, controllo non autorizzato dell'infrastruttura di ricarica e corruzione dei dati della rete di ricarica riportati al backend.

Descrizione Originale (EN): WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.

Cosa può succedere?

Un attaccante non autenticato potrebbe impersonare una stazione di ricarica, manipolando i dati inviati al backend e inviando comandi non autorizzati. Ciò potrebbe causare interruzioni gravi dei servizi di ricarica, dati di fatturazione errati e significative perdite finanziarie e reputazionali per l'azienda.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.13% (Percentile: 0.33) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare rigorose regole di firewall e liste di controllo degli accessi (ACL) per gli endpoint WebSocket OCPP. Restringere l'accesso unicamente alle reti interne e agli host autorizzati, impedendo a entità esterne o non fidate di raggiungere direttamente tali endpoint e mitigarne l'impersonificazione non autorizzata.

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:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27028 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazione non autorizzata delle stazioni e manipolare i dati inviati al backend. Un attaccante non autenticato può connettersi all'endpoint WebSocket OCPP utilizzando un identificatore di stazione di ricarica noto o scoperto, quindi inviare o ricevere comandi OCPP come un caricatore legittimo. Dato che non è richiesta alcuna autenticazione, ciò può portare a escalation dei privilegi, controllo non autorizzato dell'infrastruttura di ricarica e corruzione dei dati della rete di ricarica riportati al backend.

Descrizione Originale (EN): WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.

Cosa può succedere?

Un attaccante può impersonare le stazioni di ricarica e manipolare i dati inviati al backend, ottenendo il controllo non autorizzato delle operazioni. Questo può causare interruzioni del servizio, errori di fatturazione, perdite finanziarie e danni significativi alla reputazione aziendale.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.18% (Percentile: 0.39) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un API Gateway o un reverse proxy robusto di fronte agli endpoint WebSocket OCPP. Questo componente infrastrutturale dovrebbe imporre meccanismi di autenticazione e autorizzazione, come l'autenticazione tramite certificati client o token, prima di inoltrare le richieste al backend, fungendo da strato protettivo esterno.

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:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27767 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazione non autorizzata delle stazioni e manipolare i dati inviati al backend. Un attaccante non autenticato può connettersi all'endpoint WebSocket OCPP utilizzando un identificatore di stazione di ricarica noto o scoperto, quindi inviare o ricevere comandi OCPP come un caricatore legittimo. Dato che non è richiesta alcuna autenticazione, ciò può portare a escalation dei privilegi, controllo non autorizzato dell'infrastruttura di ricarica e corruzione dei dati della rete di ricarica riportati al backend.

Descrizione Originale (EN): WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.

Cosa può succedere?

Un attaccante non autenticato può impersonare le stazioni di ricarica, manipolando i dati e i comandi inviati al backend. Ciò può portare a interruzioni del servizio, transazioni fraudolente e la compromissione dell'intera infrastruttura di ricarica, causando perdite finanziarie e danni reputazionali.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.13% (Percentile: 0.33) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare una rigorosa segmentazione della rete per isolare gli endpoint WebSocket OCPP critici. Assicurarsi che questi endpoint siano accessibili solo da reti interne fidate o tramite VPN, impedendo l'esposizione diretta a Internet e limitando drasticamente la superficie di attacco per gli attaccanti non autenticati.

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:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27772 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazione non autorizzata delle stazioni e manipolare i dati inviati al backend. Un attaccante non autenticato può connettersi all'endpoint WebSocket OCPP utilizzando un identificatore di stazione di ricarica noto o scoperto, quindi inviare o ricevere comandi OCPP come un caricatore legittimo. Dato che non è richiesta alcuna autenticazione, ciò può portare a escalation dei privilegi, controllo non autorizzato dell'infrastruttura di ricarica e corruzione dei dati della rete di ricarica riportati al backend.

Descrizione Originale (EN): WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discovered charging station identifier, then issue or receive OCPP commands as a legitimate charger. Given that no authentication is required, this can lead to privilege escalation, unauthorized control of charging infrastructure, and corruption of charging network data reported to the backend.

Cosa può succedere?

Un attaccante può impersonare stazioni di ricarica legittime e manipolare i dati inviati al backend. Ciò consente interruzioni del servizio di ricarica, frodi finanziarie o la compromissione dell'intero sistema di gestione delle stazioni.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.13% (Percentile: 0.33) Disponibili 3 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolate i server che espongono gli endpoint WebSocket OCPP critici in una rete segmentata (ad esempio, una VLAN dedicata o una DMZ). Configurate regole di firewall stringenti per consentire l'accesso a questi endpoint solo da indirizzi IP e sistemi specifici e autorizzati all'interno dell'infrastruttura, bloccando ogni tentativo di connessione da fonti esterne o non fidate.

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:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27495 - CVSS 9.4 (CRITICA)

n8n è una piattaforma open source di automazione dei workflow. Prima delle versioni 2.10.1, 2.9.3 e 1.123.22, un utente autenticato con permessi di creazione o modifica dei workflow poteva sfruttare una vulnerabilità nel sandbox del JavaScript Task Runner per eseguire codice arbitrario al di fuori del confine del sandbox. Su istanze che utilizzano Task Runners interni (modalità runner predefinita), ciò potrebbe comportare il compromesso completo dell'host n8n. Su istanze che utilizzano Task Runners esterni, l'attaccante potrebbe ottenere accesso o influenzare altri task eseguiti sul Task Runner. I Task Runners devono essere abilitati utilizzando 'N8N_RUNNERS_ENABLED=true'. Il problema è stato risolto nelle versioni 2.10.1, 2.9.3 e 1.123.22 di n8n. Gli utenti dovrebbero aggiornare a una di queste versioni o successive per mitigare la vulnerabilità. Se l'aggiornamento non è immediatamente possibile, gli amministratori dovrebbero considerare le seguenti mitigazioni temporanee. Limitare i permessi di creazione e modifica dei workflow solo a utenti completamente affidabili e/o utilizzare la modalità runner esterno ('N8N_RUNNERS_MODE=external') per ridurre la superficie di attacco. Queste soluzioni temporanee non risolvono completamente il rischio e dovrebbero essere adottate solo come misure di mitigazione a breve termine.

Descrizione Originale (EN): n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, an authenticated user with permission to create or modify workflows could exploit a vulnerability in the JavaScript Task Runner sandbox to execute arbitrary code outside the sandbox boundary. On instances using internal Task Runners (default runner mode), this could result in full compromise of the n8n host. On instances using external Task Runners, the attacker might gain access to or impact other task executed on the Task Runner. Task Runners must be enabled using 'N8N_RUNNERS_ENABLED=true'. The issue has been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to one of these versions or later to remediate the vulnerability. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only, and/or use external runner mode ('N8N_RUNNERS_MODE=external') to limit the blast radius. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.

Cosa può succedere?

Un utente malintenzionato autenticato può ottenere il controllo completo del server n8n. Ciò consente il furto di dati sensibili gestiti dai workflow, la manipolazione o l'interruzione dei servizi aziendali critici e la potenziale compromissione di altri sistemi interni all'azienda.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.06% (Percentile: 0.17) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolate l'istanza n8n in una rete segmentata dedicata, con regole firewall restrittive che permettano solo il traffico strettamente necessario. Questo limiterà il raggio d'azione di un eventuale attaccante che riuscisse a eseguire codice arbitrario, impedendogli di accedere facilmente ad altri sistemi critici dell'infrastruttura.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** low
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27577 - CVSS 9.4 (CRITICA)

n8n è una piattaforma open source di automazione dei workflow. Prima delle versioni 2.10.1, 2.9.3 e 1.123.22, sono state identificate e corrette vulnerabilità aggiuntive nell'evaluation delle espressioni di n8n, a seguito di CVE-2025-68613. Un utente autenticato con permessi di creazione o modifica dei workflow poteva abusare di espressioni manipolate nei parametri del workflow per innescare l'esecuzione non intenzionata di comandi di sistema sull'host che esegue n8n. I problemi sono stati risolti nelle versioni 2.10.1, 2.9.3 e 1.123.22 di n8n. Gli utenti dovrebbero aggiornare a una di queste versioni o successive per mitigare tutte le vulnerabilità note. Se l'aggiornamento non è immediatamente possibile, gli amministratori dovrebbero considerare le seguenti mitigazioni temporanee. Limitare i permessi di creazione e modifica dei workflow solo a utenti pienamente affidabili e/o distribuire n8n in un ambiente rinforzato con privilegi di sistema operativo e accesso di rete limitati, al fine di ridurre l'impatto di eventuali exploit. Queste soluzioni temporanee non eliminano completamente il rischio e devono essere utilizzate solo come misure di mitigazione a breve termine.

Descrizione Originale (EN): n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, additional exploits in the expression evaluation of n8n have been identified and patched following CVE-2025-68613. An authenticated user with permission to create or modify workflows could abuse crafted expressions in workflow parameters to trigger unintended system command execution on the host running n8n. The issues have been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to one of these versions or later to remediate all known vulnerabilities. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only, and/or deploy n8n in a hardened environment with restricted operating system privileges and network access to reduce the impact of potential exploitation. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.

Cosa può succedere?

Un utente autenticato con intenzioni malevole, o un account compromesso, potrebbe sfruttare questa vulnerabilità per eseguire comandi arbitrari e ottenere il pieno controllo del server che ospita n8n. Questo permetterebbe il furto di dati sensibili, la compromissione di altri sistemi aziendali e l'interruzione dei servizi vitali.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.09% (Percentile: 0.25) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Considerando che la vulnerabilità sfrutta utenti autenticati con permessi elevati, implementare rigorosi controlli di accesso basati sul principio del privilegio minimo per la piattaforma n8n. Limitare l'autorizzazione alla creazione o modifica dei workflow solo al personale essenziale e monitorare attivamente le attività di questi account privilegiati per identificare eventuali comportamenti sospetti.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** low
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27497 - CVSS 9.4 (CRITICA)

n8n è una piattaforma open source di automazione dei workflow. Prima delle versioni 2.10.1, 2.9.3 e 1.123.22, un utente autenticato con permessi per creare o modificare workflow poteva sfruttare la modalità query SQL del nodo Merge per eseguire codice arbitrario e scrivere file arbitrari sul server n8n. I problemi sono stati corretti nelle versioni 2.10.1, 2.9.3 e 1.123.22 di n8n. Gli utenti dovrebbero aggiornare a una di queste versioni o successive per mitigare tutte le vulnerabilità note. Se l'aggiornamento non è immediatamente possibile, gli amministratori dovrebbero considerare le seguenti mitigazioni temporanee. Limitare i permessi di creazione e modifica dei workflow solo a utenti pienamente affidabili e/o disabilitare il nodo Merge aggiungendo 'n8n-nodes-base.merge' alla variabile d'ambiente 'NODES_EXCLUDE'. Questi workaround non risolvono completamente il rischio e devono essere utilizzati solo come misure di mitigazione a breve termine.

Descrizione Originale (EN): n8n is an open source workflow automation platform. Prior to versions 2.10.1, 2.9.3, and 1.123.22, an authenticated user with permission to create or modify workflows could leverage the Merge node's SQL query mode to execute arbitrary code and write arbitrary files on the n8n server. The issues have been fixed in n8n versions 2.10.1, 2.9.3, and 1.123.22. Users should upgrade to one of these versions or later to remediate all known vulnerabilities. If upgrading is not immediately possible, administrators should consider the following temporary mitigations. Limit workflow creation and editing permissions to fully trusted users only, and/or disable the Merge node by adding 'n8n-nodes-base.merge' to the 'NODES_EXCLUDE' environment variable. These workarounds do not fully remediate the risk and should only be used as short-term mitigation measures.

Cosa può succedere?

Un utente malintenzionato autenticato potrebbe prendere il pieno controllo del server n8n, compromettendo l'intera piattaforma di automazione. Questo potrebbe portare al furto di dati sensibili gestiti dai workflow, all'interruzione dei servizi e all'accesso non autorizzato ad altri sistemi aziendali.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.06% (Percentile: 0.17) Disponibili 4 valori storici
Pubblicata:	25/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementate rigorosi controlli di accesso basati sul principio del privilegio minimo per gli utenti di n8n. Limitate drasticamente il numero di utenti autenticati con permessi per creare o modificare workflow, assicurando che solo il personale strettamente necessario abbia tali privilegi elevati. Questo ridurrà significativamente la superficie di attacco e il rischio di sfruttamento della vulnerabilità.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** low
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

89: **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: SQL injection, SQLi

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2025-15498 - CVSS 9.3 (CRITICA)

Pro3W CMS è vulnerabile ad attacchi di SQL injection. La neutralizzazione inadeguata dell'input fornito in un modulo di login consente a un attaccante non autenticato di bypassare l'autenticazione e ottenere privilegi amministrativi. Questo problema è stato identificato nella versione 1.2.0 di questo software. A causa della mancanza di risposta da parte del fornitore, non è stato possibile determinare con precisione l'intervallo di versioni interessate, ma la vulnerabilità dovrebbe essere eliminata nelle versioni rilasciate a gennaio 2026 e successivamente.

Descrizione Originale (EN): Pro3W CMS if vulnerable to SQL injection attacks. Improper neutralization of input provided into a login form allows an unauthenticated attacker to bypass authentication and gain administrative privileges. This issue was identified in version 1.2.0 of this software. Due to lack of response from the vendor exact version range could not be determined, but the vulnerability should be eliminated in versions released in January 2026 and later.

Cosa può succedere?
Un attaccante non autenticato può ottenere pieno controllo amministrativo del CMS, permettendo il furto di dati sensibili, la manipolazione dei contenuti del sito web o la sua completa compromissione. Ciò può causare gravi interruzioni di servizio e danni reputazionali ed economici significativi per l'azienda.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.10% (Percentile: 0.28) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Per mitigare l'elevato rischio di SQL injection in assenza di una patch, implementare un Web Application Firewall (WAF) a protezione del Pro3W CMS. Il WAF dovrebbe essere configurato per ispezionare e filtrare il traffico in entrata, bloccando attivamente tentativi di SQL injection e altri attacchi comuni prima che raggiungano l'applicazione vulnerabile.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

89: **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

Probabilità di Sfruttamento: high

Termini Alternativi: SQL injection, SQLi

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27804 - CVSS 9.3 (CRITICA)

Parse Server è un backend open source che può essere distribuito su qualsiasi infrastruttura in grado di eseguire Node.js. Prima delle versioni 8.6.3 e 9.1.1-alpha.4, un attaccante non autenticato può falsificare un token di autenticazione Google con 'alg: "none"' per accedere come qualsiasi utente collegato a un account Google, senza conoscere le credenziali. Tutti i deployment con l'autenticazione Google abilitata sono interessati. La correzione nelle versioni 8.6.3 e 9.1.1-alpha.4 prevede di codificare l'algoritmo 'RS256' previsto invece di fidarsi dell'intestazione JWT, e sostituisce il fetcher di chiavi personalizzato dell'adapter Google con 'jwks-rsa', che rifiuta gli ID di chiave sconosciuti. Come workaround, disabilitare l'autenticazione Google fino a quando non sarà possibile eseguire l'upgrade.

Descrizione Originale (EN): Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.3 and 9.1.1-alpha.4, an unauthenticated attacker can forge a Google authentication token with 'alg: 'none"' to log in as any user linked to a Google account, without knowing their credentials. All deployments with Google authentication enabled are affected. The fix in versions 8.6.3 and 9.1.1-alpha.4 hardcodes the expected 'RS256' algorithm instead of trusting the JWT header, and replaces the Google adapter's custom key fetcher with 'jwks-rsa' which rejects unknown key IDs. As a workaround, dsable Google authentication until upgrading is possible.

Cosa può succedere?

Un attaccante non autenticato potrebbe accedere a qualsiasi account utente collegato tramite Google, senza conoscerne le credenziali. Ciò potrebbe causare furto di dati sensibili, manipolazione di informazioni o esecuzione di azioni non autorizzate a nome dell'utente compromesso.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 4 valori storici
Pubblicata:	26/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un Web Application Firewall (WAF) o un API Gateway davanti al Parse Server per ispezionare e bloccare le richieste di autenticazione Google. Configurare regole specifiche per intercettare e rifiutare qualsiasi token JWT che specifichi 'alg: "none"' nell'header, prevenendo l'exploit di falsificazione del token.

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

327: **Use of a Broken or Risky Cryptographic Algorithm**

Probabilità di Sfruttamento: high

345: **Insufficient Verification of Data Authenticity**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-2750 - CVSS 9.1 (CRITICA)

vulnerabilità di Validazione Input Impropria in Centreon Centreon Open Tickets sul Server Centrale su Linux (moduli Centreon Open Tickets). Questo problema riguarda Centreon Open Tickets sul Server Centrale: da tutte le versioni precedenti al 25.10; 24.10; 24.04.

Descrizione Originale (EN): Improper Input Validation vulnerability in Centreon Centreon Open Tickets on Central Server on Linux (Centreon Open Tickets modules).This issue affects Centreon Open Tickets on Central Server: from all before 25.10; 24.10;24.04.

Cosa può succedere?

Un aggressore potrebbe ottenere il controllo completo del server centrale Centreon, compromettendo l'intera infrastruttura di monitoraggio. Ciò potrebbe portare al furto di dati sensibili, alla manipolazione delle informazioni operative e a significative interruzioni dei servizi aziendali.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	0.04% (Percentile: 0.11) Disponibili 2 valori storici
Pubblicata:	27/02/2026
Modificata:	27/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) davanti al server Centreon. Configurare il WAF per ispezionare e filtrare attentamente il traffico in ingresso, bloccando proattivamente tentativi di iniezione di codice o altri input malevoli che potrebbero sfruttare la vulnerabilità di validazione.

CVSS Metrics

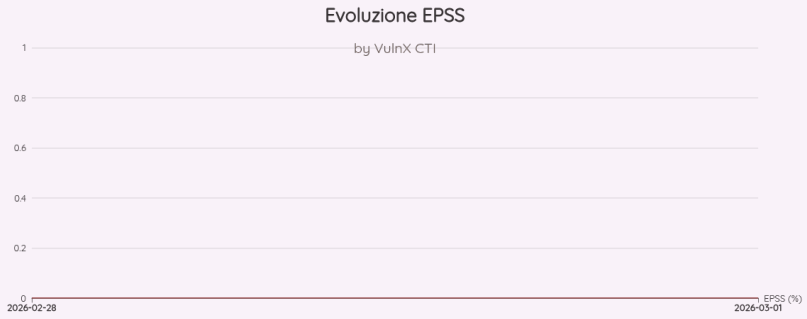
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** high
- **Interazione Utente:** none
- **Ambito:** changed
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

20: **Improper Input Validation**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



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-2020-7796 KEV

CVSS: 9.8/10 **EPSS:** 93.5% **Target:** Unknown **Rischio:** 9.7/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica a causa del suo punteggio CVSS di 9.8, dell'altissima probabilità di exploit (EPSS 93.5%) e del suo stato di vulnerabilità attivamente sfruttata (CISA KEV), rendendola un rischio immediato e concreto.

Minaccia #2: CVE-2025-49113 KEV

CVSS: 9.9/10 **EPSS:** 90.4% **Target:** Unknown **Rischio:** 9.7/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché, con un CVSS di 9.9 e un EPSS del 90.4%, è una vulnerabilità di elevatissima gravità e probabilità di sfruttamento, già attivamente sfruttata e inclusa nel CISA KEV.

Minaccia #3: CVE-2024-43468 KEV

CVSS: 9.8/10 **EPSS:** 84.6% **Target:** Unknown **Rischio:** 9.4/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché il suo punteggio CVSS di 9.8 e l'elevata probabilità di sfruttamento (EPSS 84.6%) indicano una vulnerabilità severa, già attivamente sfruttata come confermato dal CISA KEV.

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