VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Settimanale

23/02/2026 - 02/03/2026

Generato il: **02/03/2026 10:18**

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.

Indice

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

2 Note Metodologiche **7**

3 Analisi delle Debolezze (CWE) **8**
3.1 Distribuzione CWE 8
3.2 Analisi Approfondita delle Debolezze (CWE) 8
3.3 CVE del Periodo Analizzato 13

4 Vulnerabilità Critiche **63**

5 Top 3 Minacce della Settimana **63**
5.1 EPSS Elevato (>95%) 64
5.2 Raccomandazioni 65
5.3 Risorse Aggiuntive 65

1 Sommario Esecutivo

INDICATORE DI RISCHIO SETTIMANALE

ALTO

Riepilogo Settimanale Livello di Minaccia:
Questa settimana sono state registrate 961 nuove CVE, di cui 156 classificate come critiche (CVSS 9.0+) e 341 come ad alta gravità (CVSS 7.0-8.9). Sono stati aggiunti 3 nuovi exploit al catalogo KEV (Known Exploited Vulnerabilities), mentre nessuna CVE ha mostrato un punteggio EPSS (Exploit Prediction Scoring System) superiore al 50%. **Azione Consigliata:** Si raccomanda di prioritizzare immediatamente la mitigazione delle 3 vulnerabilità presenti nel catalogo KEV e delle 156 CVE critiche. È inoltre fondamentale monitorare attentamente le 341 CVE ad alta gravità per potenziali attività di exploit e pianificare le patch di conseguenza.

Metrica	Valore
Totale CVE	**961**
Critiche	**156**
Alte	**341**
EPSS >50%	**0**
KEV	**3**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	959	–
CVE Modificate	2,848	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	156	16.6%
Alte (7.0-8.9)	341	36.4%
Medie (4.0-6.9)	376	40.1%
Basse (0.1-3.9)	64	6.8%
Indicatori di Rischio		
KEV (Exploit Attivi)	3	0.3%
EPSS Elevato (>50%)	0	0.0%

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

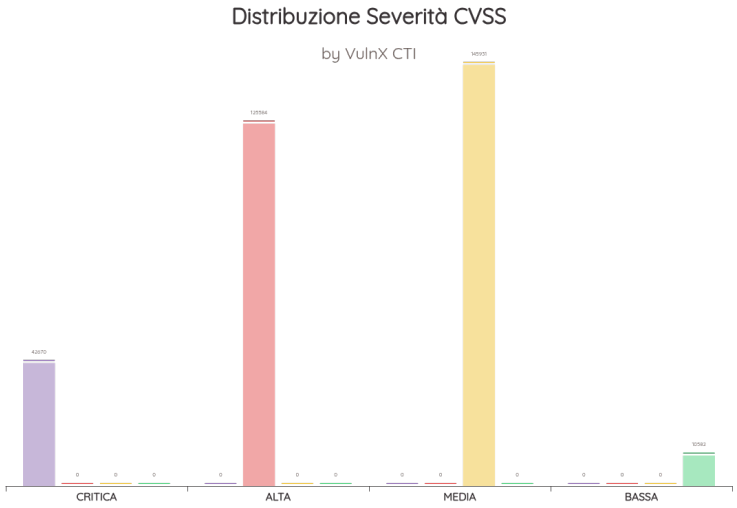
1.2 Panoramica Database (Storico Completo)

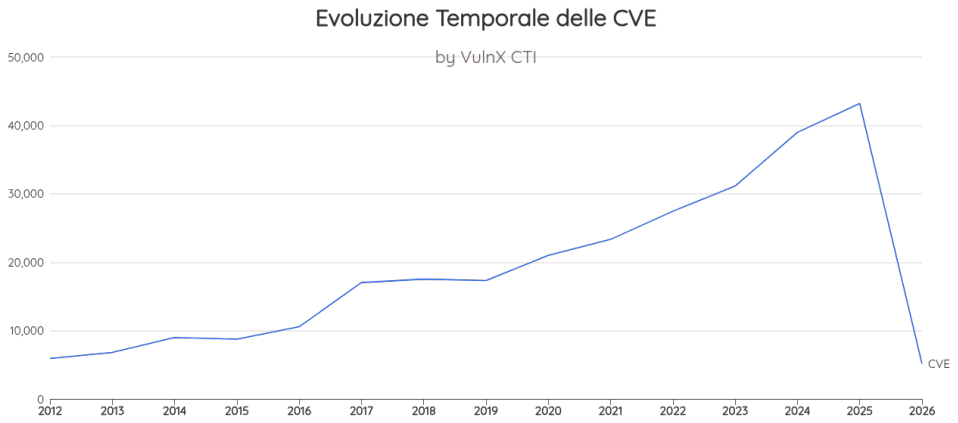
Statistiche complete del database storico su tutte le CVE mai pubblicate:

- **CVE Totali nel Database:** 335,257
- **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:

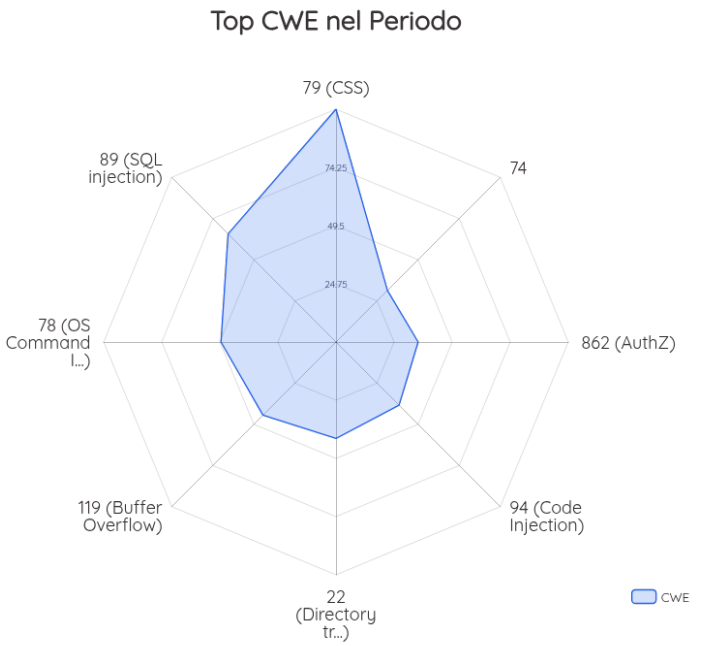


Figura 1: *Distribuzione Top CWE - Grafico Radar*

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:** 65

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per mitigare la debolezza CWE-89 (SQL Injection):
- N/A**Pratiche di Sviluppo:**Utilizzare query parametrizzate o prepared statements per tutte le interazioni con il database, evitando la concatenazione diretta di stringhe per costruire le query SQL.
- N/A**Controlli di Sviluppo:**Implementare una validazione rigorosa degli input lato server per tutti i dati forniti dall'utente, verificando tipo, formato, lunghezza e intervallo consentito, e rifiutando o sanificando input non validi.
- N/A**Strumenti di Sicurezza:**Configurare un Web Application Firewall (WAF) per rilevare e bloccare tentativi di SQL Injection a livello di rete/applicazione, aggiungendo un ulteriore strato di difesa.

119

Improper Restriction of Operations within the Bounds of a Memory Buffer

- **Occorrenze:** 44

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-119:
- N/A**Pratiche di Sviluppo:**Utilizzare funzioni di libreria sicure (es. 'strncpy_s', 'snprintf' in C/C++) ed eseguire sempre il controllo dei limiti (bounds checking) durante tutte le operazioni sui buffer per prevenire scritture fuori dai confini.
- N/A**Configurazioni di Sicurezza:**Abilitare le protezioni a livello di compilatore (es. stack canaries, ASLR) e di sistema operativo (DEP/NX) per mitigare l'impatto e la sfruttabilità degli overflow di buffer.
- N/A**Controlli di Rete/Sviluppo:**Implementare una validazione rigorosa e centralizzata dell'input a tutti i livelli dell'applicazione (front-end, back-end, API) per prevenire l'invio di dati malevoli o di dimensioni eccessive che potrebbero causare overflow.

22

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

▶ **Occorrenze:** 41

Raccomandazioni di Difesa

▶ Ecco 3 raccomandazioni specifiche e attuabili per mitigare la debolezza CWE-22 (Path Traversal):

▶ N/A**Implementare una rigorosa validazione degli input:**Per tutti i parametri utilizzati nella costruzione di percorsi di file, applicare una**whitelist**di caratteri e percorsi consentiti. Negare esplicitamente sequenze di directory traversal (‘../‘, ‘..\{}‘, ‘%2e%2e%2f‘, ecc.) e le loro codifiche URL.

▶ N/A**Configurare regole WAF avanzate:**Utilizzare un**WAF (Web Application Firewall)**per rilevare e bloccare proattivamente pattern comuni di attacchi di path traversal nelle richieste HTTP, anche prima che raggiungano l’applicazione.

▶ N/A**Canonicalizzare i percorsi e verificare l’ambito:**Prima di accedere a qualsiasi risorsa basata su percorsi forniti dall’utente,**canonicalizzare il percorso**(es. ‘java.nio.file.Path.normalize()‘ o ‘os.path.abspath()‘ in Python) e verificare che il percorso risolto ricada sempre all’interno della directory base prevista, impedendo l’accesso a directory esterne.

74

Improper Neutralization of Special Elements in Output Used by a Downstream Component (’Injection’)

▶ **Occorrenze:** 31

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-74:
- N/A**Implementare la validazione dell'input (lato server) basata su whitelist e la codifica dell'output contestuale**per tutti i dati forniti dall'utente prima dell'elaborazione o della visualizzazione.
- N/A**Adottare query parametrizzate o prepared statements**per tutte le interazioni con il database, evitando la concatenazione diretta di stringhe SQL.
- N/A**Configurare regole WAF (Web Application Firewall)**per rilevare e mitigare attacchi di injection noti (es. SQLi, XSS) al perimetro della rete.

120

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

- **Occorrenze:** 23

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-120:
- N/A**Pratiche di Sviluppo:**Utilizzare funzioni di gestione della memoria e delle stringhe sicure (es. 'strncpy_s', 'snprintf' in C/C++, 'std::string' in C++) e implementare una rigorosa validazione degli input per tutti i dati forniti dall'utente, verificando e limitando la dimensione.
- N/A**Configurazioni di Sicurezza (OS/Compilatore):**Abilitare e configurare le protezioni a livello di sistema operativo come ASLR (Address Space Layout Randomization) e DEP (Data Execution Prevention), e le stack canaries del compilatore, per mitigare l'impatto di eventuali overflow.
- N/A**Strumenti di Sicurezza (SDLC):**Integrare strumenti SAST (Static Application Security Testing) nel ciclo di sviluppo (CI/CD) per identificare proattivamente le vulnerabilità di buffer overflow nel codice sorgente prima del deployment.

476

NULL Pointer Dereference

▶ **Occorrenze:** 21

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e pratiche per mitigare la debolezza CWE-476 (NULL Pointer Dereference):
- N/A**Controlli espliciti dei puntatori:**Implementare sempre controlli espliciti per verificare che un puntatore non sia NULL prima di dereferenziarlo, specialmente dopo operazioni di allocazione di memoria o input/output che potrebbero restituire un puntatore non valido.
- N/A**Adozione di smart pointer:**Nei linguaggi che li supportano (es. C++), utilizzare smart pointer (come ‘std::unique_ptr‘ o ‘std::shared_ptr‘) per automatizzare la gestione della memoria e ridurre significativamente il rischio di dereferenziazioni di puntatori NULL o dangling.
- N/A**Integrazione SAST:**Implementare l’analisi statica del codice (SAST) nella pipeline CI/CD per rilevare automaticamente potenziali dereferenziazioni di puntatori NULL e altri errori di gestione della memoria durante le fasi di sviluppo e test.

3.3 CVE del Periodo Analizzato

Trovate **959** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **25** CVE:

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, compromettendo tutti i dati e i sistemi ospitati. Questo porterebbe al furto di informazioni sensibili (es. dati di donatori e beneficiari) e alla potenziale interruzione totale dei servizi dell'organizzazione, con gravi danni reputazionali e finanziari.

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:
Isolare il server che ospita l'applicazione WeGIA in una rete segmentata o DMZ dedicata. Implementare regole firewall restrittive per consentire solo il traffico strettamente necessario, limitando così la superficie di attacco e impedendo movimenti laterali 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 completo del sistema affetto senza autenticazione. Ciò permette il furto di dati sensibili, l'interruzione dei servizi critici e la potenziale compromissione dell'intera rete aziendale.

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:
Isolare immediatamente il dispositivo Copeland XWEB Pro in un segmento di rete dedicato e altamente ristretto. Implementare regole firewall stringenti per limitare tutto il traffico di rete in entrata e in uscita ai soli servizi essenziali e a sorgenti fidate, riducendo al minimo l'esposizione sia a minacce esterne che interne.

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 possono ottenere il controllo completo del server web, portando al furto di dati sensibili, all'interruzione dei servizi essenziali o all'uso del server come trampolino di lancio per ulteriori attacchi interni. In alternativa, potrebbero esporre il codice sorgente di applicazioni critiche, compromettendo la proprietà intellettuale aziendale.

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:
In assenza di una patch, implementare un Web Application Firewall (WAF) o un reverse proxy davanti al server TinyWeb vulnerabile. Questo permetterà di ispezionare e filtrare le richieste HTTP/HTTPS, bloccando tentativi di bypass dei controlli sui parametri CGI prima che raggiungano il server. Tale misura agisce come un controllo compensativo critico per mitigare l'esecuzione di codice remoto e la divulgazione di sorgenti.

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 pieno controllo del server Centreon centrale. Questo permetterebbe il furto di dati sensibili, la manipolazione dei sistemi monitorati e la potenziale interruzione critica dei servizi aziendali.

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:
Isolare immediatamente il server centrale Centreon, che ospita i moduli Open Tickets vulnerabili, in un segmento di rete dedicato (VLAN). Implementare regole firewall stringenti per consentire l'accesso a tale server e al servizio Centreon solo dagli host e dagli utenti strettamente necessari e autorizzati, minimizzando così la superficie d'attacco e il potenziale impatto.

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?

L'exploit di questa vulnerabilità critica può permettere a un attaccante di eseguire comandi non autorizzati sui sistemi interessati. Ciò comporta il rischio di un completo compromesso del sistema, con conseguente furto di dati sensibili, interruzione dei servizi essenziali o la possibilità di lanciare ulteriori attacchi all'interno della rete aziendale.

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:

Implementare un rigoroso principio del minimo privilegio per il servizio o l'applicazione OpenClaw, confinandone l'esecuzione in un ambiente isolato (ad esempio, un container o un ambiente chroot). Assicurarsi che tale ambiente abbia accesso limitato solo ai comandi e ai percorsi di sistema strettamente necessari, riducendo drasticamente l'impatto di eventuali esecuzioni non autorizzate anche in caso di bypass della validazione interna.

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'esecuzione riuscita permetterebbe agli attaccanti di rubare chiavi API e token sensibili, ottenendo accesso non autorizzato a sistemi correlati e dati critici. Potrebbero inoltre iniettare codice malevolo nel repository, compromettendo la piattaforma OpenLIT e rischiando interruzioni del servizio o attacchi alla supply chain.

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:

Implementare controlli di accesso con il principio del minimo privilegio per tutti i workflow di GitHub Actions che utilizzano l'evento 'pull_request_target'. Assicurarsi che questi workflow operino con le autorizzazioni e gli ambiti strettamente necessari, in particolare per l'accesso in scrittura al repository, l'accesso ai segreti e i privilegi di deployment. Questo ridurrà significativamente il raggio d'azione di un potenziale attacco in caso di esecuzione di codice non affidabile.

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-2026-3422 - 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 aggressore remoto può ottenere il controllo completo del server U-Office Force. Ciò permette il furto di dati riservati, l'interruzione dei servizi essenziali e la diffusione dell'attacco all'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 immediatamente i server U-Office Force in un segmento di rete dedicato, applicando rigorose regole di firewall per limitare l'accesso solo alle fonti e ai protocolli strettamente necessari. Questo ridurrà significativamente la superficie di attacco e conterrà potenziali compromissioni da attori remoti 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

502: **Deserialization of Untrusted Data**

Probabilità di Sfruttamento: medium

Termini Alternativi: Marshaling, Unmarshaling, PHP Object Injection, Pickling, Unpickling

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?

Un attaccante non autenticato potrebbe ottenere il controllo completo dei sistemi interessati, installando software malevolo. Ciò potrebbe portare al furto di dati sensibili, alla diffusione di ransomware con conseguente blocco delle operazioni aziendali, o alla compromissione 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:
Implementare regole di firewall rigorose sui sistemi che eseguono IDExpert Windows Logon Agent. Queste regole dovrebbero limitare l'accesso in entrata e, soprattutto, in uscita, consentendo solo le connessioni essenziali per il funzionamento legittimo dell'agente e bloccando i tentativi di scaricare file da sorgenti remote 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-2026-2999 - 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?

Gli attaccanti remoti possono ottenere il controllo completo dei sistemi aziendali, installare software malevolo e rubare dati sensibili. Ciò può causare interruzioni operative critiche, significative perdite finanziarie e gravi danni alla reputazione 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 una rete segmentata dedicata. Implementare rigorose regole firewall per limitare le connessioni in uscita da questi sistemi, consentendo il traffico solo verso destinazioni essenziali e fidate. Questo preverrà il download e l'esecuzione di file arbitrari da sorgenti remote 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-2026-28411 - 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 può ottenere pieno controllo delle aree amministrative dell'applicazione WeGIA, consentendo l'accesso non autorizzato a dati sensibili e la potenziale manipolazione o furto di informazioni critiche. Ciò può causare interruzioni operative significative e gravi danni alla reputazione dell'organizzazione.

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:

Isolate il server dell'applicazione WeGIA all'interno di un segmento di rete dedicato (DMZ) con regole firewall restrittive. Configurate il firewall per consentire l'accesso solo da indirizzi IP fidati o zone di rete specifiche necessarie per gli utenti legittimi, riducendo drasticamente l'esposizione agli attaccanti non autenticati.

CVSS Metrics

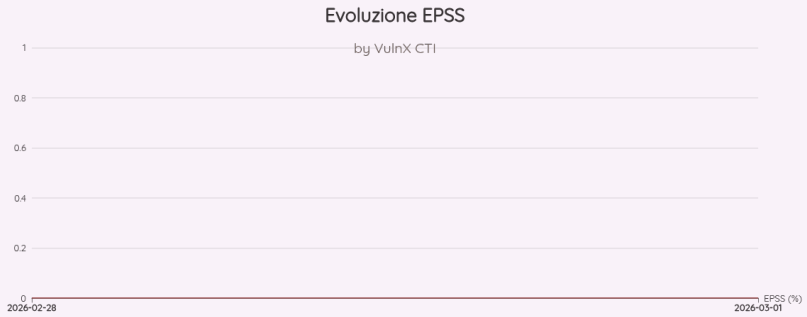
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

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-2026-28408 - 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 attaccante potrebbe accedere a funzionalità riservate ai dipendenti, permettendo il furto di dati sensibili e l'iniezione di informazioni non autorizzate o dannose. Ciò comprometterebbe gravemente l'integrità e la riservatezza delle operazioni, con potenziali interruzioni dei servizi o danni alla reputazione aziendale.

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 un Web Application Firewall (WAF) per bloccare l'accesso diretto allo script 'adicionar_tipo_docs_atendido.php' o per imporre un'autenticazione aggiuntiva a livello di perimetro. Configurare regole che neghino le richieste non autorizzate a questo percorso specifico, mitigando l'exploit a monte dell'applicazione e fornendo un controllo di accesso compensativo.

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-2026-28268 - 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?

Se sfruttata, questa vulnerabilità permette a un attaccante di reimpostare le password degli utenti e ottenere accesso non autorizzato ai loro account Vikunja. Ciò può portare al furto o alla compromissione di dati sensibili relativi a progetti e attività aziendali, con gravi conseguenze per la privacy e la sicurezza operativa.

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:
Implementare un monitoraggio robusto sugli endpoint API di Vikunja, tracciando attentamente le richieste di reset password e i successivi tentativi di login. Configurare avvisi per schemi sospetti, come molteplici reset password per lo stesso utente da indirizzi IP insoliti o l'uso di token di reset già impiegati. Questo consente di rilevare e rispondere rapidamente a potenziali tentativi 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

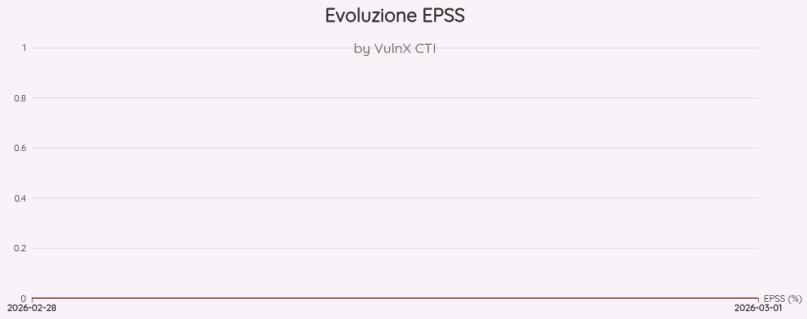
459: **Incomplete Cleanup**

Termini Alternativi: Insufficient Cleanup

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

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-27751 - 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?

Sfruttando questa vulnerabilità, un attaccante remoto otterrebbe il controllo amministrativo completo del dispositivo, potendo così interrompere i servizi critici, accedere a dati sensibili o compromettere l'intera rete aziendale. Ciò esporrebbe l'azienda a gravi rischi operativi, perdite finanziarie e danni alla reputazione.

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:

Per mitigare questa vulnerabilità critica, isolare l'interfaccia di gestione del dispositivo SODOLA SL902-SWTGW124AS all'interno di una VLAN o segmento di rete dedicato e strettamente controllato. Implementare rigorose regole di firewall per consentire l'accesso a tale interfaccia *esclusivamente* da workstation amministrative autorizzate e indirizzi IP specifici, bloccando ogni altro tentativo 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

1392: **Use of Default Credentials**

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?

Gli attaccanti potrebbero ottenere accesso completo e non autorizzato ai dispositivi compromessi. Questo permetterebbe loro di rubare dati sensibili, interrompere servizi critici o compromettere l'intera 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:

Isolare l'interfaccia di gestione del dispositivo SODOLA SL902-SWTGW124AS in una VLAN di gestione dedicata e strettamente segmentata. Implementare stringenti liste di controllo degli accessi (ACL) sui firewall per consentire l'accesso a tale interfaccia unicamente da host amministrativi specifici e autorizzati. Questa misura riduce significativamente la superficie di attacco e la capacità di attori malevoli di sfruttare la vulnerabilità di falsificazione delle sessioni.

CVSS Metrics

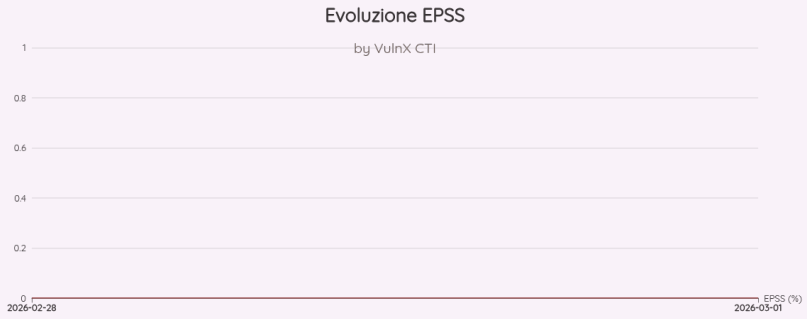
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

330: **Use of Insufficiently Random Values**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-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?

Lo sfruttamento di questa vulnerabilità critica consente agli aggressori di accedere, rubare o manipolare dati aziendali sensibili, come informazioni sui clienti e finanziarie. Ciò può portare a gravi interruzioni operative, perdite finanziarie e danni alla reputazione dell'azienda.

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 un Web Application Firewall (WAF) in fronte all'applicazione Windesk.Fm per ispezionare e filtrare il traffico HTTP/S in ingresso. Configurare il WAF con regole robuste e aggiornate specificamente mirate a rilevare e bloccare tentativi di SQL Injection, agendo come uno scudo protettivo essenziale per mitigare questa vulnerabilità critica in assenza di 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

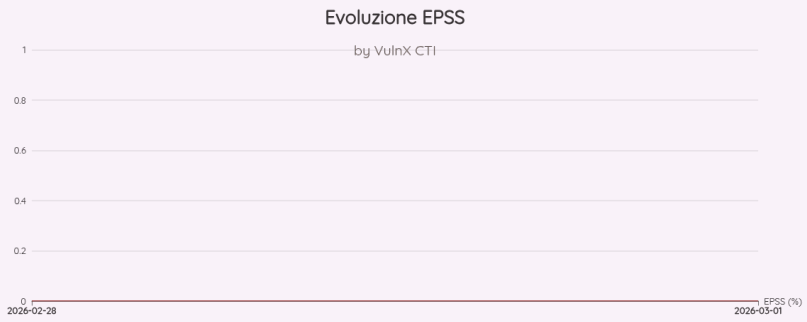
CWE - Common Weakness Enumeration

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-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 potrebbe assumere il controllo della sessione di un utente autenticato, ottenendo accesso non autorizzato al CMS. Ciò potrebbe portare al furto di dati sensibili, alla modifica del contenuto del sito web o alla completa compromissione del sistema, causando gravi interruzioni e danni alla reputazione.

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:

Implementare un Web Application Firewall (WAF) o un reverse proxy configurato per richiedere una ri-autenticazione o un secondo fattore di autenticazione (MFA) per l'accesso alle aree amministrative o alle funzionalità critiche del CMS. Questo ridurrebbe significativamente il rischio che un attaccante possa sfruttare una sessione fissa per eseguire azioni privilegiate, anche in assenza di una patch 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:** 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?

Un attaccante potrebbe rubare dati sensibili di clienti e aziendali, inclusi dettagli finanziari e informazioni personali. Potrebbe anche ottenere il controllo completo del database, manipolando o cancellando dati critici e causando interruzioni significative alla piattaforma e-commerce.

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 e bloccare proattivamente i tentativi di SQL Injection. Configurare il WAF con regole robuste per rilevare e prevenire attacchi noti, fornendo una protezione immediata a livello di infrastruttura. Questo fungerà da controllo compensativo critico 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-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?
Gli attaccanti possono ottenere il controllo completo dei sistemi Xerox FreeFlow Core vulnerabili, permettendo il furto di dati sensibili, l'interruzione dei servizi critici o l'installazione di software dannoso. Questo può causare gravi perdite finanziarie e danni alla reputazione aziendale.

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:
Isolate i server Xerox FreeFlow Core su un segmento di rete dedicato (VLAN) e implementate regole firewall restrittive. Consentite l'accesso a tali sistemi solo da indirizzi IP e utenti strettamente autorizzati e necessari, minimizzando così la superficie di attacco e il potenziale impatto di una 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 remoto può ottenere il pieno controllo dei dispositivi Totolink vulnerabili, compromettendo l'intera rete aziendale. Ciò comporta un elevato rischio di furto di dati sensibili, interruzione dei servizi critici e ulteriori attacchi alla infrastruttura IT.

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 VLAN di gestione dedicata, applicando rigorose regole di firewall per limitare l'accesso alla sua interfaccia web di amministrazione esclusivamente da indirizzi IP fidati interni alla rete di gestione. Questo minimizzerà l'esposizione e preverrà attacchi remoti non autorizzati all'interfaccia vulnerabile.

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

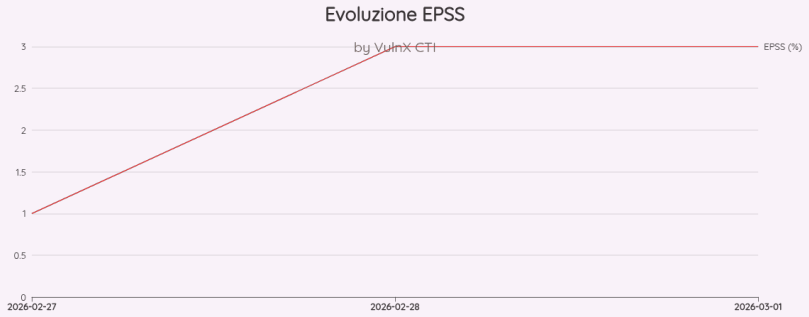
Termini Alternativi: Command injection

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-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 WordPress. Ciò consente di rubare dati sensibili, interrompere i servizi, iniettare contenuti dannosi o compromettere completamente la presenza online dell'azienda.

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 Web Application Firewall (WAF) a livello infrastrutturale per filtrare e bloccare le richieste HTTP maliziose. Configurare il WAF per ispezionare le richieste di registrazione utente e bloccare proattivamente quelle che tentano di manipolare il parametro 'user_role' o di assegnare ruoli privilegiati, come 'Administrator', durante il processo di registrazione.

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-2026-28213 - 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 ottenere il controllo completo degli account utente sulle piattaforme EverShop, accedendo ai dati sensibili dei clienti, inclusi i dettagli degli ordini e le informazioni personali. Ciò può portare a frodi finanziarie, gravi violazioni della privacy e un significativo danno alla reputazione dell'azienda.

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 e configurare un Web Application Firewall (WAF) a protezione dell'applicazione EverShop. Il WAF dovrebbe essere impostato per ispezionare le risposte dell'API, in particolare per la funzionalità "Password Dimenticata", bloccando o sanificando quelle che espongono token di reset password o altre informazioni sensibili. Questo offre un livello di controllo compensativo per prevenire la fuoriuscita di dati critici.

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?

Gli attaccanti non autenticati possono ottenere il controllo completo del sistema, permettendo il furto, la modifica o la cancellazione di dati sensibili. Questo include la possibilità di interrompere i servizi essenziali e utilizzare il sistema come punto di partenza per ulteriori attacchi alla rete 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:
Implementare un Web Application Firewall (WAF) o un API Gateway davanti all'istanza di OpenViking. Configurare il WAF/Gateway per intercettare e bloccare tutte le richieste dirette agli endpoint amministrativi senza una preventiva autenticazione o autorizzazione rigorosa, mitigando così l'accesso non autenticato.

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 ospita ZenTaoPMS. Ciò consentirebbe loro di rubare dati sensibili, interrompere i servizi critici o utilizzare il server compromesso per lanciare ulteriori attacchi all'interno della rete aziendale.

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 una rigorosa segmentazione di rete, isolando il server ZenTaoPMS in una DMZ o un VLAN dedicato. Configurare regole firewall restrittive per limitare l'accesso in entrata solo alle porte essenziali e bloccare le connessioni in uscita non autorizzate. Questo ridurrà significativamente il potenziale impatto di una compromissione, impedendo la movimentazione laterale degli attaccanti.

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 potrebbe ottenere il pieno controllo del server che esegue Langflow. Ciò consentirebbe il furto di dati sensibili, l'interruzione dei servizi critici o l'installazione di malware, compromettendo gravemente l'intera infrastruttura aziendale.

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:

Eseguire l'applicazione Langflow in un ambiente containerizzato o sandbox con privilegi minimi assoluti. Limitare rigorosamente le capacità del container, come l'accesso al filesystem e le connessioni di rete, per contenere l'impatto di un'eventuale esecuzione di codice arbitrario e prevenire l'accesso a risorse di sistema sensibili.

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?

Sfruttando questa vulnerabilità, un attaccante potrebbe ottenere il controllo completo dei sistemi affetti. Ciò potrebbe portare al furto di dati sensibili, all’interruzione dei servizi critici o all’ulteriore compromissione 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:

Isolare i sistemi che utilizzano FreeRDP in una rete segmentata, limitando l’accesso alle porte RDP (tipicamente TCP 3389) tramite firewall esclusivamente da indirizzi IP o sottoreti predefinite e strettamente autorizzate. Questo riduce drasticamente la superficie di attacco, impedendo a entità non autorizzate di raggiungere il servizio vulnerabile.

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

4 Vulnerabilità Critiche

5 Top 3 Minacce della Settimana

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

Minaccia #1: CVE-2026-20127 KEV

CVSS: 10.0/10 **EPSS:** 2.2% **Target:** Unknown **Rischio:** 7.1/10

Perché è una minaccia prioritaria:
Questo rappresenta una minaccia critica perché ha un punteggio CVSS massimo (10.0) ed è attivamente sfruttato a livello globale, come indicato dalla sua inclusione nel catalogo CISA KEV.

Minaccia #2: CVE-2026-25108 KEV

CVSS: 8.8/10 **EPSS:** 18.6% **Target:** Unknown **Rischio:** 6.8/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché è attivamente sfruttata (CISA KEV), indicando un rischio immediato, e possiede un elevato punteggio CVSS di 8.8/10 con un'alta probabilità di exploit (EPSS 18.6%).

Minaccia #3: CVE-2026-27597

CVSS: 10.0/10 **EPSS:** 0.4% **Target:** Unknown **Rischio:** 6.0/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché il suo punteggio CVSS di 10.0 indica una vulnerabilità di massima gravità, probabilmente sfruttabile da remoto e senza autenticazione. Nonostante la bassa probabilità di exploit attuale (EPSS 0.4%) e l'assenza dal catalogo KEV, la gravità massima implica un elevato rischio di compromissione completa una volta che lo sfruttamento diventerà più diffuso.

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