VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Settimanale

02/03/2026 - 09/03/2026

Generato il: **09/03/2026 07:05**

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

INDICATORE DI RISCHIO SETTIMANALE

ALTO

Riepilogo Settimanale Livello di Minaccia:
Questa settimana sono state identificate 1443 nuove CVE, di cui 197 classificate come critiche e 581 ad alta gravità. L'aggiunta di 7 nuove vulnerabilità al catalogo CISA KEV e la presenza di una vulnerabilità con un punteggio EPSS superiore al 50% indicano un rischio elevato di sfruttamento attivo. **Azione Consigliata:** Prioritizzare immediatamente la mitigazione delle 7 CVE presenti nel catalogo KEV e della singola CVE con EPSS superiore al 50%. Mantenere un monitoraggio costante sulle vulnerabilità critiche e ad alta gravità per prevenire potenziali compromissioni.

Metrica	Valore
Totale CVE	**1443**
Critiche	**197**
Alte	**581**
EPSS >50%	**1**
KEV	**7**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	1,437	–
CVE Modificate	1,638	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	197	15.3%
Alte (7.0-8.9)	581	45.1%
Medie (4.0-6.9)	463	35.9%
Basse (0.1-3.9)	47	3.6%
Indicatori di Rischio		
KEV (Exploit Attivi)	7	0.5%
EPSS Elevato (>50%)	1	0.1%

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

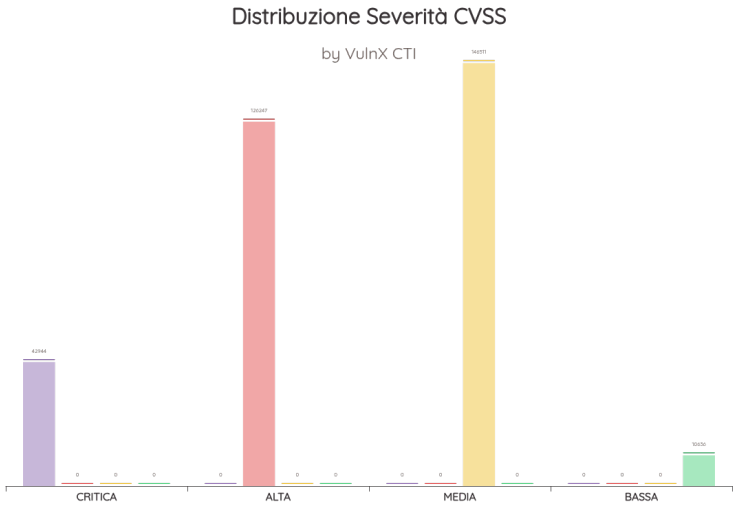
1.2 Panoramica Database (Storico Completo)

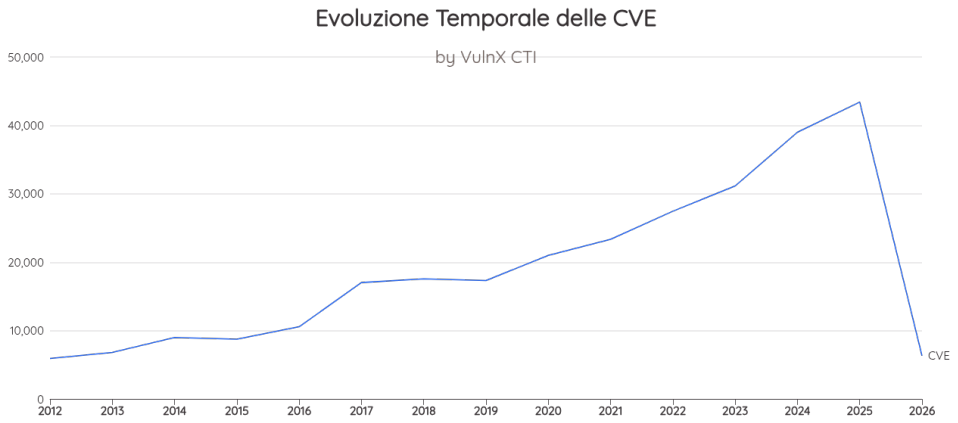
Statistiche complete del database storico su tutte le CVE mai pubblicate:

- **CVE Totali nel Database:** 336,688
- **KEV Totali (Vulnerabilità con Exploit Noti):** 1,538
- **CWE Totali Catalogate:** 969
- **CPE Totali Monitorati:** 2,231,399

Severità	Conteggio	Percentuale
CRITICA	42,944	13.2%
ALTA	126,247	38.7%
MEDIA	146,511	44.9%
BASSA	10,636	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:

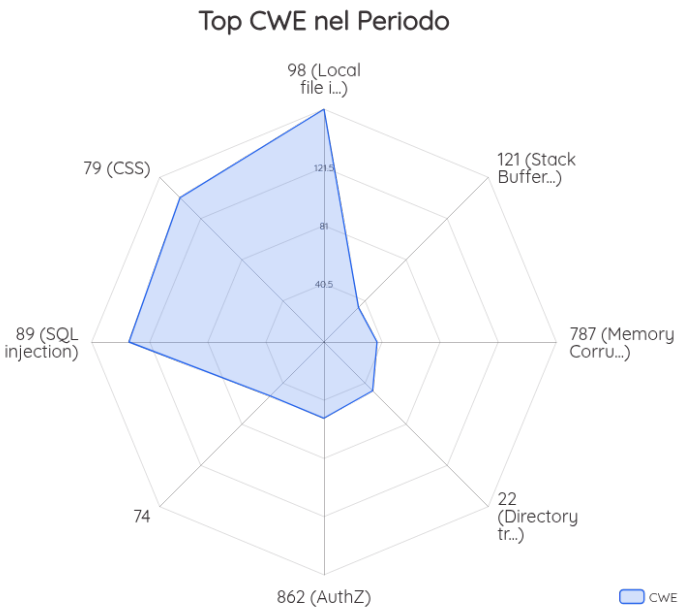


Figura 1: *Distribuzione Top CWE - Grafico Radar*

3.2 Analisi Approfondita delle Debolezze (CWE)

Le debolezze più comuni con raccomandazioni di difesa.

74

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

▶ **Occorrenze:** 53

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-74:
- N/A**Pratiche di Sviluppo:**Utilizzare query parametrizzate o prepared statements per tutti gli accessi ai database, evitando la concatenazione diretta di stringhe SQL con input utente. Implementare una rigorosa validazione dell'input lato server (es. whitelist, tipizzazione forte) per tutti i dati forniti dall'utente.
- N/A**Pratiche di Sviluppo:**Applicare l'encoding contestuale all'output prima di renderizzarlo nelle pagine web o di inviarlo a componenti a valle, per neutralizzare elementi speciali che potrebbero essere interpretati erroneamente (es. HTML entity encoding per XSS).
- N/A**Strumenti/Configurazioni di Sicurezza:**Configurare un Web Application Firewall (WAF) con regole specifiche per rilevare e bloccare proattivamente tentativi di injection (es. SQLi, XSS, Command Injection) basandosi su firme e analisi euristica del traffico.

121

Stack-based Buffer Overflow

- **Occorrenze:** 34

Raccomandazioni di Difesa

- Ecco 2 raccomandazioni specifiche e attuabili per CWE-121:
- N/A**Pratiche di Sviluppo:**Utilizzare funzioni di libreria sicure per la gestione della memoria e delle stringhe (es. 'strncpy', 'snprintf' in C/C++) e implementare controlli rigorosi sui limiti dei buffer per prevenire scritture fuori dai limiti.
- N/A**Configurazioni di Sicurezza:**Abilitare le protezioni a livello di compilatore (es. Stack Canaries, tramite flag come '-fstack-protector' o '/GS') e a livello di sistema operativo (es. DEP/NX - Data Execution Prevention/No-Execute, ASLR - Address Space Layout Randomization).

284

Improper Access Control

▶ **Occorrenze:** 32

Raccomandazioni di Difesa

▶ Ecco 3 raccomandazioni specifiche e attuabili per CWE-284 - Improper Access Control:

▶ N/A**Implementare e applicare rigorosamente il controllo degli accessi basato sui ruoli (RBAC) o sugli attributi (ABAC) a livello applicativo**, garantendo che ogni richiesta di accesso alle risorse sia verificata rispetto alle autorizzazioni dell'utente o del servizio.

▶ N/A**Adottare il principio del privilegio minimo (Least Privilege)**per tutti gli utenti, i servizi e i sistemi, concedendo solo le autorizzazioni strettamente necessarie per svolgere le proprie funzioni.

▶ N/A**Implementare la segmentazione della rete e configurare regole firewall restrittive**per limitare la connettività tra i diversi componenti del sistema e le zone di rete, aggiungendo un livello di controllo d'accesso a livello infrastrutturale.

119

Improper Restriction of Operations within the Bounds of a Memory Buffer

▶ **Occorrenze:** 30

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-119:
- N/A**Pratiche di Sviluppo:**Implementare controlli rigorosi sui limiti (bounds checking) per tutte le operazioni su buffer e utilizzare esclusivamente funzioni di gestione della memoria sicure (es. ‘snprintf‘, ‘memcpy_s‘), evitando funzioni a rischio come ‘strcpy‘ o ‘sprintf‘.
- N/A**Strumenti/Configurazioni di Sicurezza:**Configurare i compilatori per abilitare protezioni come gli stack canaries (‘-fstack-protector‘ in GCC/Clang) e l’Address Sanitizer (ASan) per rilevare e mitigare gli overflow di buffer in fase di compilazione e runtime.
- N/A**Controlli di Rete:**Configurare regole WAF (Web Application Firewall) per limitare la dimensione massima degli input e dei parametri HTTP, bloccando richieste che superano soglie predefinite per prevenire tentativi di sfruttamento di buffer overflow.

434

Unrestricted Upload of File with Dangerous Type

- **Occorrenze:** 28

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-434:
- N/A**Validazione lato server con whitelist:**Implementare una validazione lato server rigorosa che accetti solo estensioni di file da una whitelist di tipi sicuri (es. .jpg, .png, .pdf) e ne verifichi il tipo MIME effettivo e i ”magic bytes” per prevenire spoofing.
- N/A**Archiviazione sicura e disabilitazione esecuzione:**Archiviare i file caricati in una directory dedicata non accessibile direttamente via web e configurare il server (es. Apache, Nginx, IIS) per disabilitare esplicitamente l’esecuzione di script (es. PHP, ASP, JSP) in tale percorso.
- N/A**Regole WAF avanzate:**Configurare regole WAF (Web Application Firewall) per rilevare e bloccare proattivamente caricamenti di file con estensioni pericolose, doppiamente estese (es. .jpg.php) o contenuti indicativi di web shell e script malevoli.

266

Incorrect Privilege Assignment

▶ **Occorrenze:** 20

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-266 (Incorrect Privilege Assignment):
- N/A**Implementare il principio del minimo privilegio (Least Privilege Principle):**Assicurarsi che utenti, servizi e applicazioni abbiano solo le autorizzazioni strettamente necessarie per svolgere le proprie funzioni, e non di più.
- N/A**Adottare il controllo degli accessi basato sui ruoli (RBAC - Role-Based Access Control):**Definire ruoli con insiemi specifici di permessi e assegnare utenti o gruppi a tali ruoli, anziché concedere permessi individuali.
- N/A**Effettuare revisioni periodiche e audit degli accessi e dei privilegi assegnati:**Verificare regolarmente che le autorizzazioni siano ancora appropriate e rimuovere tempestivamente quelle non più necessarie o eccessive.

3.3 CVE del Periodo Analizzato

Trovate **1437** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **25** CVE:

CVE-2026-3630 - CVSS 9.8 (CRITICA)

Delta Electronics COMMGR2 presenta una vulnerabilità di Stack-based Buffer Overflow.

Descrizione Originale (EN): Delta Electronics COMMGR2 has Stack-based Buffer Overflow vulnerability.

Cosa può succedere?
L'exploit di questa vulnerabilità critica potrebbe portare al controllo completo dei sistemi Delta Electronics COMMGR2. Ciò permetterebbe agli attaccanti di rubare dati sensibili, interrompere le operazioni o manipolare processi industriali critici con gravi conseguenze.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	09/03/2026
Modificata:	09/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Per mitigare il rischio elevato di questa vulnerabilità critica, isolare i sistemi Delta Electronics COMMGR2 vulnerabili in una rete segmentata e protetta (ad esempio, una DMZ o una zona OT dedicata). Implementare regole firewall stringenti per limitare l'accesso solo alle porte e ai protocolli strettamente necessari da host autorizzati, minimizzando così la superficie di attacco e prevenendo la propagazione di eventuali compromissioni.

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

Approfondisci su VulnX

CVE-2026-3703 - CVSS 9.8 (CRITICA)

È stata riscontrata una vulnerabilità in Wavlink NU516U1 251208. Questa interessa la funzione sub_401A10 del file /cgi-bin/login.cgi. Manipolando l'argomento ipaddr è possibile causare un out-of-bounds write. L'attacco può essere eseguito da remoto. L'exploit è stato pubblicato e può essere utilizzato. Si raccomanda di aggiornare il componente interessato. Il fornitore è stato contattato tempestivamente, ha risposto in modo molto professionale e ha rilasciato rapidamente una versione corretta del prodotto interessato.

Descrizione Originale (EN): A flaw has been found in Wavlink NU516U1 251208. This affects the function sub_401A10 of the file /cgi-bin/login.cgi. Executing a manipulation of the argument ipaddr can lead to out-of-bounds write. The attack may be performed from remote. The exploit has been published and may be used. Upgrading the affected component is recommended. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Cosa può succedere?

Sfruttando questa grave vulnerabilità, un attaccante remoto può ottenere il controllo completo del dispositivo Wavlink. Ciò potrebbe portare al furto di dati aziendali, alla compromissione dell'intera rete e all'interruzione dei servizi essenziali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.07% (Percentile: 0.20)
Pubblicata:	08/03/2026
Modificata:	08/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare il dispositivo Wavlink NU516U1 in una VLAN o segmento di rete strettamente controllato. Implementare regole firewall per limitare l'accesso alla sua interfaccia di gestione (es. porte 80/443) esclusivamente agli indirizzi IP autorizzati della rete di amministrazione, minimizzando l'esposizione a potenziali attaccanti remoti.

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

119: **Improper Restriction of Operations within the Bounds of a Memory Buffer**

Probabilità di Sfruttamento: high

Termini Alternativi: Buffer Overflow, buffer overrun, memory safety

---

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

Probabilità di Sfruttamento: high

Termini Alternativi: Memory Corruption

Approfondisci su VulnX

CVE-2026-3802 - CVSS 8.8 (ALTA)

È stata individuata una vulnerabilità in Tenda i3 1.0.0.6(2204). La funzione interessata da questo problema è formexeCommand del file /goform/exeCommand. L'esecuzione di una manipolazione dell'argomento cmdinput può portare a un buffer overflow basato su stack. L'attacco può essere eseguito da remoto. L'exploit è stato divulgato pubblicamente e può essere utilizzato.

Descrizione Originale (EN): A vulnerability was determined in Tenda i3 1.0.0.6(2204). Affected by this issue is the function formexeCommand of the file /goform/exeCommand. Executing a manipulation of the argument cmdinput can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.

Cosa può succedere?
Sfruttando questa vulnerabilità, un attaccante remoto può ottenere il controllo completo del dispositivo Tenda i3. Questo espone l'azienda a rischi significativi come l'interruzione dei servizi, la sottrazione di informazioni riservate e la possibilità di attacchi a sistemi interni.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	09/03/2026
Modificata:	09/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolare il dispositivo Tenda i3 vulnerabile in un segmento di rete dedicato, come una VLAN di gestione o una DMZ, per limitare la sua esposizione. Implementare rigorose regole firewall per consentire l'accesso alla sua interfaccia amministrativa solo da host fidati e specifici all'interno della rete, bloccando ogni altro tentativo di connessione esterna o interna non autorizzata.

CVSS Metrics

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

CWE - Common Weakness Enumeration

119: **Improper Restriction of Operations within the Bounds of a Memory Buffer**

Probabilità di Sfruttamento: high

Termini Alternativi: Buffer Overflow, buffer overrun, memory safety

---

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Buffer Overflow, Stack Overflow

Approfondisci su VulnX

CVE-2026-3769 - CVSS 8.8 (ALTA)

È stata rilevata una vulnerabilità in Tenda F453 1.0.0.3. La funzione interessata da questo problema è WrlclientSet del file /goform/WrlclientSet. La manipolazione dell'argomento GO provoca un overflow del buffer basato su stack. L'attacco può essere eseguito da remoto. L'exploit è ora pubblico e potrebbe essere utilizzato.

Descrizione Originale (EN): A vulnerability was detected in Tenda F453 1.0.0.3. Affected by this issue is the function WrlclientSet of the file /goform/WrlclientSet. The manipulation of the argument GO results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.

Cosa può succedere?
Un attaccante remoto può ottenere il controllo completo dei dispositivi Tenda vulnerabili, compromettendo la sicurezza della rete aziendale. Questo potrebbe causare gravi interruzioni dei servizi, furto di dati sensibili e l'accesso non autorizzato a sistemi interni.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	08/03/2026
Modificata:	08/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolare il dispositivo Tenda F453 in un segmento di rete dedicato (es. VLAN o DMZ) per limitare la superficie di attacco e il potenziale impatto di una compromissione. Implementare regole firewall stringenti per restringere il traffico in ingresso e in uscita da tale segmento solo a quello strettamente indispensabile per le sue funzionalità essenziali.

CVSS Metrics

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

CWE - Common Weakness Enumeration

119: **Improper Restriction of Operations within the Bounds of a Memory Buffer**

Probabilità di Sfruttamento: high

Termini Alternativi: Buffer Overflow, buffer overrun, memory safety

---

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Buffer Overflow, Stack Overflow

Approfondisci su VulnX

CVE-2026-3799 - CVSS 8.8 (ALTA)

È stata individuata una vulnerabilità in Tenda i3 1.0.0.6(2204). Questa riguarda la funzione formSetCfm del file /goform/setcfm. La manipolazione dell'argomento funcpara1 provoca un overflow del buffer basato su stack. È possibile un'esecuzione remota dell'attacco. L'exploit è stato pubblicato e può essere utilizzato.

Descrizione Originale (EN): A flaw has been found in Tenda i3 1.0.0.6(2204). This impacts the function formSetCfm of the file /goform/setcfm. This manipulation of the argument funcpara1 causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.

Cosa può succedere?

Un attaccante può ottenere il controllo completo dei dispositivi interessati, consentendo l'accesso non autorizzato alla rete aziendale. Questo può portare al furto di dati sensibili, all'interruzione dei servizi critici e all'uso del dispositivo compromesso come punto di partenza per ulteriori attacchi interni.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	09/03/2026
Modificata:	09/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Data l'assenza di una patch e la possibilità di esecuzione remota, si raccomanda di isolare immediatamente il dispositivo Tenda i3 in un segmento di rete dedicato. Implementare controlli di accesso rigorosi tramite firewall, consentendo il traffico solo da indirizzi IP e porte strettamente essenziali per la sua gestione, limitando drasticamente la superficie d'attacco.

CVSS Metrics

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

CWE - Common Weakness Enumeration

119: **Improper Restriction of Operations within the Bounds of a Memory Buffer**

Probabilità di Sfruttamento: high

Termini Alternativi: Buffer Overflow, buffer overrun, memory safety

---

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Buffer Overflow, Stack Overflow

Approfondisci su VulnX

CVE-2026-3801 - CVSS 8.8 (ALTA)

È stata scoperta una vulnerabilità in Tenda i3 1.0.0.6(2204). La funzione interessata da questa vulnerabilità è formSetAutoPing del file /goform/setAutoPing. La manipolazione dell'argomento ping1/ping2 provoca un overflow del buffer basato su stack. L'attacco può essere eseguito da remoto. L'exploit è stato reso pubblico e potrebbe essere utilizzato.

Descrizione Originale (EN): A vulnerability was found in Tenda i3 1.0.0.6(2204). Affected by this vulnerability is the function formSetAutoPing of the file /goform/setAutoPing. Performing a manipulation of the argument ping1/ping2 results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made public and could be used.

Cosa può succedere?

Sfruttando questa vulnerabilità, un attaccante remoto potrebbe ottenere il controllo completo del dispositivo Tenda i3. Ciò potrebbe portare all'interruzione dei servizi di rete, al furto di dati sensibili che transitano sulla rete o all'utilizzo del dispositivo compromesso come punto di partenza per attacchi più ampi all'infrastruttura aziendale.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	09/03/2026
Modificata:	09/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare il rischio di questa vulnerabilità remota e pubblicamente sfruttabile, isolare il dispositivo Tenda i3 in un segmento di rete dedicato e strettamente controllato. Implementare regole firewall restrittive per limitare l'accesso in entrata al dispositivo solo alle sorgenti e alle porte strettamente necessarie, riducendo drasticamente la sua esposizione.

CVSS Metrics

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

CWE - Common Weakness Enumeration

119: **Improper Restriction of Operations within the Bounds of a Memory Buffer**

Probabilità di Sfruttamento: high

Termini Alternativi: Buffer Overflow, buffer overrun, memory safety

---

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Buffer Overflow, Stack Overflow

Approfondisci su VulnX

CVE-2026-28353 - CVSS 10.0 (CRITICA)

Trivy Vulnerability Scanner è un'estensione di VS Code che aiuta a individuare vulnerabilità. Nella versione 1.8.12 dell'Estensione Trivy per VSCode, distribuita tramite il marketplace OpenVSX, è stato compromesso e conteneva codice dannoso progettato per sfruttare un agente di coding AI locale al fine di raccogliere ed esfiltrare informazioni sensibili. Si consiglia agli utenti che utilizzano l'artefatto interessato di rimuoverlo immediatamente e di ruotare i segreti dell'ambiente. L'artefatto dannoso è stato rimosso dal marketplace. Non sono stati identificati altri artefatti interessati.

Descrizione Originale (EN): Trivy Vulnerability Scanner is a VS Code extension that helps find vulnerabilities. In Trivy VSCode Extension version 1.8.12, which was distributed via OpenVSX marketplace was compromised and contained malicious code designed to leverage local AI coding agent to collect and exfiltrate sensitive information. Users using the affected artifact are advised to immediately remove it and rotate environment secrets. The malicious artifact has been removed from the marketplace. No other affected artifacts have been identified.

Cosa può succedere?

Lo sfruttamento di questa vulnerabilità critica potrebbe causare il furto di dati sensibili, inclusi codici sorgente e credenziali, direttamente dagli ambienti di sviluppo. Ciò comporta un grave rischio di compromissione della proprietà intellettuale, interruzione delle operazioni e danni significativi alla reputazione aziendale.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.04% (Percentile: 0.13) Disponibili 3 valori storici
Pubblicata:	05/03/2026
Modificata:	05/03/2026
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 rigorosa segmentazione della rete per isolare le workstation degli sviluppatori in una zona dedicata e ad alto rischio. Configurare firewall con regole di egress filtering stringenti per limitare il traffico in uscita da queste zone, consentendo solo le connessioni essenziali e bloccando i tentativi di esfiltrazione dati non autorizzati verso l'esterno.

CVSS Metrics

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

CWE - Common Weakness Enumeration

506: **Embedded Malicious Code**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-0848 - CVSS 10.0 (CRITICA)

Le versioni di NLTK <=3.9.2 sono vulnerabili a esecuzione di codice arbitrario a causa di una validazione inappropriata degli input nel modulo StanfordSegmenter. Il modulo carica dinamicamente file .jar Java esterni senza verifica o sandboxing. Un attaccante può fornire o sostituire il file JAR, consentendo l'esecuzione di bytecode Java arbitrario al momento dell'importazione. Questa vulnerabilità può essere sfruttata tramite metodi come poisoning del modello, attacchi MITM o poisoning delle dipendenze, portando all'esecuzione di codice remoto. Il problema deriva dall'esecuzione diretta del file JAR tramite subprocess con un classpath non validato, permettendo a classi dannose di essere eseguite quando caricate dalla JVM.

Descrizione Originale (EN): NLTK versions <=3.9.2 are vulnerable to arbitrary code execution due to improper input validation in the StanfordSegmenter module. The module dynamically loads external Java .jar files without verification or sandboxing. An attacker can supply or replace the JAR file, enabling the execution of arbitrary Java bytecode at import time. This vulnerability can be exploited through methods such as model poisoning, MITM attacks, or dependency poisoning, leading to remote code execution. The issue arises from the direct execution of the JAR file via subprocess with unvalidated classpath input, allowing malicious classes to execute when loaded by the JVM.

Cosa può succedere?
Un aggressore potrebbe ottenere il controllo totale dei sistemi che utilizzano le versioni vulnerabili di NLTK. Ciò permetterebbe il furto di dati sensibili, l'interruzione dei servizi critici o l'installazione di malware, come ransomware, con gravi conseguenze operative e finanziarie per l'azienda.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.41% (Percentile: 0.61) Disponibili 3 valori storici
Pubblicata:	05/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare rigorosi controlli di accesso ai file system per le directory che contengono i file .jar utilizzati dal modulo StanfordSegmenter di NLTK. Assicurarsi che solo gli account di sistema autorizzati e con privilegi minimi possano modificare o scrivere in queste posizioni, prevenendo l'introduzione o la sostituzione di file JAR malevoli e quindi l'esecuzione di codice arbitrario.

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

20: **Improper Input Validation**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-30861 - CVSS 9.9 (CRITICA)

WeKnora è un framework alimentato da LLM progettato per una comprensione approfondita dei documenti e il recupero semantico. Dalla versione 0.2.5 fino prima della versione 0.2.10, esiste una vulnerabilità di esecuzione remota di codice (RCE) non autenticata nella convalida della configurazione MCP stdio. L'applicazione consente la registrazione utente senza restrizioni, il che significa che qualsiasi attaccante può creare un account ed sfruttare la falla di command injection. Nonostante l'implementazione di una whitelist per i comandi consentiti (npx, uvx) e di blacklist per argomenti e variabili di ambiente pericolose, la convalida può essere aggirata utilizzando il flag -p con npx node. Ciò consente a qualsiasi attaccante di eseguire comandi arbitrari con i privilegi dell'applicazione, portando a un compromesso completo del sistema. Questo problema è stato risolto nella versione 0.2.10.

Descrizione Originale (EN): WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. From version 0.2.5 to before version 0.2.10, an unauthenticated remote code execution (RCE) vulnerability exists in the MCP stdio configuration validation. The application allows unrestricted user registration, meaning any attacker can create an account and exploit the command injection flaw. Despite implementing a whitelist for allowed commands (npx, uvx) and blacklists for dangerous arguments and environment variables, the validation can be bypassed using the -p flag with npx node. This allows any attacker to execute arbitrary commands with the application's privileges, leading to complete system compromise. This issue has been patched in version 0.2.10.

Cosa può succedere?

Un attaccante potrebbe ottenere il pieno controllo dei server che eseguono WeKnora, consentendo il furto, la manipolazione o la distruzione di dati sensibili e l'interruzione completa dei servizi. Ciò può causare gravi perdite finanziarie, danni alla reputazione e compromettere l'intera infrastruttura aziendale.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.21% (Percentile: 0.43)
Pubblicata:	07/03/2026
Modificata:	07/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un Web Application Firewall (WAF) davanti all'applicazione WeKnora. Configurare il WAF per rilevare e bloccare proattivamente i pattern di attacco noti associati all'esecuzione remota di codice (RCE), creando una barriera protettiva contro tentativi di sfruttamento non autenticati.

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

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

Approfondisci su VulnX

CVE-2026-30860 - CVSS 9.9 (CRITICA)

WeKnora è un framework alimentato da LLM progettato per una comprensione approfondita dei documenti e il recupero semantico. Prima della versione 0.2.12, esiste una vulnerabilità di remote code execution (RCE) nella funzionalità di query del database dell'applicazione. Il sistema di validazione non riesce a ispezionare ricorsivamente i nodi figli all'interno delle espressioni array e delle espressioni row di PostgreSQL, consentendo agli attaccanti di bypassare le protezioni contro SQL injection. Smugglando funzioni pericolose di PostgreSQL all'interno di queste espressioni e concatenandole con operazioni su large object e capacità di caricamento di librerie, un attaccante non autenticato può ottenere l'esecuzione di codice arbitrario sul server del database con privilegi dell'utente del database. Questo problema è stato risolto nella versione 0.2.12.

Descrizione Originale (EN): WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.12, a remote code execution (RCE) vulnerability exists in the application's database query functionality. The validation system fails to recursively inspect child nodes within PostgreSQL array expressions and row expressions, allowing attackers to bypass SQL injection protections. By smuggling dangerous PostgreSQL functions inside these expressions and chaining them with large object operations and library loading capabilities, an unauthenticated attacker can achieve arbitrary code execution on the database server with database user privileges. This issue has been patched in version 0.2.12.

Cosa può succedere?

Gli attaccanti potrebbero ottenere il controllo completo dei sistemi aziendali, rubare dati sensibili come informazioni clienti o segreti commerciali, e causare interruzioni gravi ai servizi critici. Ciò potrebbe comportare perdite finanziarie significative, danni alla reputazione e responsabilità legali.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.08% (Percentile: 0.23)
Pubblicata:	07/03/2026
Modificata:	07/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolare il framework WeKnora in un segmento di rete dedicato e strettamente controllato. Questo limiterà l'accesso non autorizzato e la potenziale propagazione di attacchi in caso di sfruttamento della vulnerabilità RCE, impedendo che un'eventuale compromissione si estenda ad altri sistemi critici dell'infrastruttura.

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

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-2026-29789 - CVSS 9.9 (CRITICA)

Vito è un'applicazione web auto-ospitata che aiuta a gestire server e distribuire applicazioni PHP sui server di produzione. Prima della versione 3.20.3, una mancanza di controllo dell'autorizzazione nelle azioni di creazione di workflow site-creation consentiva a un attaccante autenticato con accesso in scrittura ai workflow in un progetto di creare e gestire siti su server appartenenti ad altri progetti fornendo un server_id esterno. Questo problema è stato risolto nella versione 3.20.3.

Descrizione Originale (EN): Vito is a self-hosted web application that helps manage servers and deploy PHP applications into production servers. Prior to version 3.20.3, a missing authorization check in workflow site-creation actions allows an authenticated attacker with workflow write access in one project to create/manage sites on servers belonging to other projects by supplying a foreign server_id. This issue has been patched in version 3.20.3.

Cosa può succedere?

Un attaccante autenticato può creare e gestire siti su server non autorizzati, ottenendo il controllo completo di infrastrutture critiche. Questo può causare gravi interruzioni di servizio, furto o manipolazione di dati sensibili e la piena compromissione dei sistemi aziendali.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.05% (Percentile: 0.14) Disponibili 2 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementate una segmentazione di rete rigorosa, isolando i server che ospitano siti di progetti diversi in VLAN o sottoreti separate. Questo approccio limiterebbe significativamente la capacità di un attaccante, anche in caso di bypass dell'autorizzazione in Vito, di creare o gestire siti su server non appartenenti al proprio segmento di rete.

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

862: **Missing Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28466 - CVSS 9.9 (CRITICA)

OpenClaw versioni precedenti alla 2026.2.14 presentano una vulnerabilità nel gateway in cui non sanificano i campi di approvazione interna nei parametri node.invoke, consentendo ai client autenticati di bypassare il controllo di approvazione dell'esecuzione per i comandi system.run. Gli attaccanti con credenziali valide per il gateway possono iniettare campi di controllo dell'approvazione per eseguire comandi arbitrari sui host dei nodi connessi, compromettendo potenzialmente le workstation degli sviluppatori e i CI runners.

Descrizione Originale (EN): OpenClaw versions prior to 2026.2.14 contain a vulnerability in the gateway in which it fails to sanitize internal approval fields in node.invoke parameters, allowing authenticated clients to bypass exec approval gating for system.run commands. Attackers with valid gateway credentials can inject approval control fields to execute arbitrary commands on connected node hosts, potentially compromising developer workstations and CI runners.

Cosa può succedere?

Un attaccante con credenziali valide per il gateway potrebbe eseguire comandi arbitrari sui sistemi collegati, ottenendo il controllo totale di workstation o server. Ciò porterebbe al furto di dati sensibili, all'interruzione dei servizi critici e alla potenziale compromissione dell'intera rete aziendale.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.09% (Percentile: 0.26) Disponibili 3 valori storici
Pubblicata:	05/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare il gateway OpenClaw in una rete segmentata e ristretta, accessibile esclusivamente da workstation di gestione autorizzate e dedicate. Questo riduce drasticamente la superficie di attacco e limita la capacità di un eventuale aggressore di raggiungere il gateway o di sfruttare la vulnerabilità per accedere ad altri sistemi critici dell'infrastruttura.

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

863: **Incorrect Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-29058 - CVSS 9.8 (CRITICA)

AVideo è un software di piattaforma di condivisione video. Prima della versione 7.0, un attaccante non autenticato può eseguire comandi OS arbitrari sul server iniettando sostituzioni di comandi shell nel parametro GET base64Url. Ciò può portare a compromissione completa del server, esfiltrazione di dati (ad esempio, segreti di configurazione, chiavi interne, credenziali) e interruzione del servizio. Questo problema è stato corretto nella versione 7.0.

Descrizione Originale (EN): AVideo is a video-sharing Platform software. Prior to version 7.0, an unauthenticated attacker can execute arbitrary OS commands on the server by injecting shell command substitution into the base64Url GET parameter. This can lead to full server compromise, data exfiltration (e.g., configuration secrets, internal keys, credentials), and service disruption. This issue has been patched in version 7.0.

Cosa può succedere?
L'attaccante potrebbe ottenere il controllo completo del server aziendale. Questo porterebbe al furto di dati sensibili, inclusi segreti di configurazione e credenziali, e all'interruzione dei servizi essenziali dell'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.10% (Percentile: 0.27) Disponibili 3 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un Web Application Firewall (WAF) davanti al server AVideo per ispezionare e filtrare il traffico in entrata. Questo può aiutare a rilevare e bloccare tentativi di iniezione di comandi tramite il parametro 'base64Url', fungendo da controllo compensativo critico per mitigare l'esecuzione di comandi arbitrari 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

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-2026-2331 - CVSS 9.8 (CRITICA)

Un attaccante potrebbe eseguire operazioni di lettura e scrittura non autenticata su aree sensibili del filesystem tramite il Fileaccess di AppEngine via HTTP a causa di restrizioni di accesso inadeguate. Una directory critica del filesystem è stata involontariamente esposta tramite la funzione di accesso ai file basata su HTTP, consentendo l'accesso senza autenticazione. Ciò include file di parametri dei dispositivi, permettendo a un attaccante di leggere e modificare le impostazioni dell'applicazione, inclusi password definite dal cliente. Inoltre, l'esposizione della directory dell'applicazione personalizzata potrebbe consentire l'esecuzione di codice Lua arbitrario all'interno dell'ambiente sandboxed di AppEngine.

Descrizione Originale (EN): An attacker may perform unauthenticated read and write operations on sensitive filesystem areas via the AppEngine Fileaccess over HTTP due to improper access restrictions. A critical filesystem directory was unintentionally exposed through the HTTP-based file access feature, allowing access without authentication. This includes device parameter files, enabling an attacker to read and modify application settings, including customer-defined passwords. Additionally, exposure of the custom application directory may allow execution of arbitrary Lua code within the sandboxed AppEngine environment.

Cosa può succedere?

Un attaccante non autenticato potrebbe leggere e modificare aree sensibili del filesystem, inclusi i parametri di configurazione dei dispositivi. Questo consentirebbe la compromissione completa dei sistemi, il furto di dati critici e l'interruzione dei servizi aziendali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.17% (Percentile: 0.38) Disponibili 3 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
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 rigorosa segmentazione di rete per isolare l'ambiente AppEngine, assicurandosi che l'endpoint Fileaccess non sia direttamente esposto a reti non fidate (es. internet). Configurare un firewall per consentire l'accesso a tale funzionalità solo da indirizzi IP e segmenti di rete interni strettamente autorizzati e monitorati.

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

552: **Files or Directories Accessible to External Parties**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-2446 - CVSS 9.8 (CRITICA)

Il plugin PowerPack per LearnDash WordPress, prima della versione 1.3.0, non effettua controlli di autorizzazione e CRSF in un'azione AJAX, consentendo a utenti non autenticati di aggiornare opzioni arbitrarie di WordPress (come default_role, ecc.) e di creare utenti admin arbitrari.

Descrizione Originale (EN): The PowerPack for LearnDash WordPress plugin before 1.3.0 does not have authorization and CRSF checks in an AJAX action, allowing unauthenticated users to update arbitrary WordPress options (such as default_role etc) and create arbitrary admin users

Cosa può succedere?

Un attaccante può ottenere il pieno controllo amministrativo del sito WordPress, creando account admin arbitrari. Questo permette di rubare o manipolare dati sensibili, compromettere la reputazione aziendale e interrompere gravemente i servizi online.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.07% (Percentile: 0.22) Disponibili 3 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) a monte dell'installazione di WordPress. Configurare il WAF per ispezionare e bloccare attivamente le richieste che tentano di manipolare opzioni critiche di sistema o creare utenti con privilegi elevati, fungendo da strato protettivo contro tentativi di sfruttamento di vulnerabilità AJAX da parte di utenti 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

862: **Missing Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28501 - CVSS 9.8 (CRITICA)

WWBN AVideo è una piattaforma video open source. Prima della versione 24.0, esiste una vulnerabilità di SQL Injection non autenticata in AVideo all'interno dei componenti objects/videos.json.php e objects/video.php. L'applicazione non sanifica correttamente il parametro catName quando viene fornito tramite il corpo di una richiesta POST in formato JSON. Poiché l'input JSON viene analizzato e unito a $_REQUEST dopo l'esecuzione dei controlli di sicurezza globali, il payload aggira i meccanismi di sanificazione esistenti. Questo problema è stato risolto nella versione 24.0.

Descrizione Originale (EN): WWBN AVideo is an open source video platform. Prior to version 24.0, an unauthenticated SQL Injection vulnerability exists in AVideo within the objects/videos.json.php and objects/video.php components. The application fails to properly sanitize the catName parameter when it is supplied via a JSON-formatted POST request body. Because JSON input is parsed and merged into $_REQUEST after global security checks are executed, the payload bypasses the existing sanitization mechanisms. This issue has been patched in version 24.0.

Cosa può succedere?

Un attaccante non autenticato può rubare dati sensibili dal database, come informazioni sugli utenti e sui contenuti video. Questo può portare alla manipolazione o distruzione dei dati, causando interruzioni del servizio e compromettendo l'integrità della piattaforma. In casi gravi, è possibile ottenere il controllo completo del sistema.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.03% (Percentile: 0.08) Disponibili 3 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) a monte dell'applicazione AVideo. Configurare il WAF per ispezionare e filtrare attivamente le richieste POST in formato JSON, bloccando specificamente i pattern noti di SQL Injection sul parametro 'catName'. Questo fornirà un controllo compensativo fondamentale a livello di infrastruttura per prevenire lo sfruttamento della vulnerabilità non autenticata.

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-2026-21536 - CVSS 9.8 (CRITICA)

Vulnerabilità di esecuzione remota di codice nel Microsoft Devices Pricing Program

Descrizione Originale (EN): Microsoft Devices Pricing Program Remote Code Execution Vulnerability

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo dei sistemi che gestiscono il programma di prezzi Microsoft. Questo consentirebbe il furto di dati sensibili, inclusi prezzi e informazioni sui clienti, e causerebbe gravi interruzioni operative e danni finanziari all'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.40% (Percentile: 0.60) Disponibili 3 valori storici
Pubblicata:	05/03/2026
Modificata:	05/03/2026
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 che ospitano il Microsoft Devices Pricing Program in un segmento di rete dedicato e strettamente controllato. Applicare regole firewall rigorose per limitare l'accesso solo al traffico essenziale e da fonti autorizzate, riducendo drasticamente la superficie di attacco e contenendo 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

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-2026-28474 - CVSS 9.8 (CRITICA)

Le versioni precedenti del plugin Nextcloud Talk di OpenClaw fino alla 2026.2.6 accettano corrispondenza di uguaglianza sul campo display name actor.name mutabile per la validazione dell'allowlist, consentendo agli attaccanti di aggirare le allowlist di DM e stanze. Un attaccante può modificare il proprio display name di Nextcloud per corrispondere a un ID utente in allowlist e ottenere accesso non autorizzato a conversazioni riservate.

Descrizione Originale (EN): OpenClaw's Nextcloud Talk plugin versions prior to 2026.2.6 accept equality matching on the mutable actor.name display name field for allowlist validation, allowing attackers to bypass DM and room allowlists. An attacker can change their Nextcloud display name to match an allowlisted user ID and gain unauthorized access to restricted conversations.

Cosa può succedere?

Un attaccante potrebbe ottenere accesso non autorizzato a conversazioni private e stanze riservate su Nextcloud Talk, consentendo il furto di informazioni sensibili e la violazione della riservatezza aziendale. Ciò potrebbe comportare gravi danni reputazionali, finanziari e violazioni della conformità.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 3 valori storici
Pubblicata:	05/03/2026
Modificata:	05/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un monitoraggio rigoroso dei log di accesso e attività del plugin Nextcloud Talk. Configurare alert per rilevare anomalie come accessi a conversazioni o stanze riservate da parte di utenti con nomi visualizzati che non corrispondono al loro ID utente effettivo, o comportamenti sospetti che indichino un'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:** high

CWE - Common Weakness Enumeration

863: **Incorrect Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28470 - CVSS 9.8 (CRITICA)

OpenClaw nelle versioni precedenti alla 2026.2.2 contiene una vulnerabilità di bypass dell'allowlist nelle approvazioni di esecuzione (must be enabled) che consente agli attacker di eseguire comandi arbitrari tramite l'iniezione di sintassi di sostituzione dei comandi. Gli attacker possono bypassare la protezione dell'allowlist inserendo $() o backtick non escapati all'interno di stringhe tra virgolette doppie per eseguire comandi non autorizzati.

Descrizione Originale (EN): OpenClaw versions prior to 2026.2.2 contain an exec approvals (must be enabled) allowlist bypass vulnerability that allows attackers to execute arbitrary commands by injecting command substitution syntax. Attackers can bypass the allowlist protection by embedding unescaped $() or backticks inside double-quoted strings to execute unauthorized commands.

Cosa può succedere?

Un attaccante potrebbe ottenere il pieno controllo dei sistemi interessati, consentendo il furto di dati sensibili e l'interruzione delle operazioni aziendali. Potrebbe anche essere installato software malevolo, inclusi ransomware, compromettendo gravemente l'integrità dei dati e la disponibilità dei servizi.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.07% (Percentile: 0.21) Disponibili 3 valori storici
Pubblicata:	05/03/2026
Modificata:	05/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare il principio del minimo privilegio per l'applicazione OpenClaw, assicurando che il processo operi con le autorizzazioni strettamente indispensabili per le sue funzionalità. Parallelamente, rafforzare il monitoraggio dei log di sistema e delle attività di rete generate da OpenClaw per identificare tempestivamente esecuzioni di comandi anomale o tentativi di 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

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-28391 - CVSS 9.8 (CRITICA)

OpenClaw versioni precedenti alla 2026.2.2 non riescono a convalidare correttamente i metacaratteri di Windows cmd.exe nelle richieste di esecuzione con lista di autorizzazione (configurazione non predefinita), consentendo agli attaccanti di aggirare le restrizioni di approvazione dei comandi. Gli attaccanti remoti possono creare stringhe di comando con metacaratteri di shell come & o %...% per eseguire comandi non approvati oltre le operazioni consentite.

Descrizione Originale (EN): OpenClaw versions prior to 2026.2.2 fail to properly validate Windows cmd.exe metacharacters in allowlist-gated exec requests (non-default configuration), allowing attackers to bypass command approval restrictions. Remote attackers can craft command strings with shell metacharacters like & or %...% to execute unapproved commands beyond the allowlisted operations.

Cosa può succedere?

Attaccanti remoti potrebbero ottenere il controllo completo dei sistemi vulnerabili, eseguendo comandi non autorizzati. Questo permetterebbe il furto di dati critici, l'interruzione dei servizi essenziali o la compromissione dell'intera rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.05% (Percentile: 0.15) Disponibili 3 valori storici
Pubblicata:	05/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare il principio del minimo privilegio per l'account di servizio OpenClaw. Assicurarsi che l'applicazione abbia solo le autorizzazioni strettamente necessarie per svolgere le sue funzioni operative, limitando così il potenziale impatto di un'esecuzione di comandi non autorizzata o di un bypass delle restrizioni.

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-21622 - CVSS 9.5 (CRITICA)

Insufficient Session Expiration vulnerability in hexpm hexpm/hexpm ('Elixir.Hexpm.Accounts.PasswordReset' module) allows Account Takeover. I token di reset della password generati tramite il flusso "Reset your password" non scadono. Quando un utente richiede un reset della password, Hex invia un'email contenente un link di reset con un token. Questo token rimane valido indefinitamente fino all'uso. Non è applicata alcuna scadenza basata sul tempo. Se le email storiche di un utente vengono esposte tramite una violazione dei dati (ad esempio, un archivio di caselle di posta trapelato), qualsiasi email di reset della password non utilizzata contenuta in quel dataset potrebbe essere sfruttata da un attaccante per reimpostare la password della vittima. L'attaccante non necessita di accesso attuale all'account email della vittima, ma solo di una copia precedentemente trapelata dell'email di reset. Questa vulnerabilità è associata ai file di programma lib/hexpm/accounts/password_reset.ex e alle routine di programma 'Elixir.Hexpm.Accounts.PasswordReset':can_reset?/3. Il problema interessa hexpm: da 617e44c71f1dd9043870205f371d375c5c4d886d prima di bb0e42091995945deef10556f58d046a52eb7884.

Descrizione Originale (EN): Insufficient Session Expiration vulnerability in hexpm hexpm/hexpm ('Elixir.Hexpm.Accounts.PasswordReset' module) allows Account Takeover. Password reset tokens generated via the 'Reset your password' flow do not expire. When a user requests a password reset, Hex sends an email containing a reset link with a token. This token remains valid indefinitely until used. There is no time-based expiration enforced. If a user's historical emails are exposed through a data breach (e.g., a leaked mailbox archive), any unused password reset email contained in that dataset could be used by an attacker to reset the victim's password. The attacker does not need current access to the victim's email account, only access to a previously leaked copy of the reset email. This vulnerability is associated with program files lib/hexpm/accounts/password_reset.ex and program routines 'Elixir.Hexpm.Accounts.PasswordReset':can_reset?/3. This issue affects hexpm: from 617e44c71f1dd9043870205f371d375c5c4d886d before bb0e42091995945deef10556f58d046a52eb7884.

Cosa può succedere?

Un aggressore potrebbe ottenere il controllo completo degli account utente. Ciò potrebbe causare il furto di dati aziendali sensibili, interruzioni di servizio e gravi danni alla reputazione dell'azienda.

Punteggio CVSS:	9.5 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 3 valori storici
Pubblicata:	05/03/2026
Modificata:	05/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Per mitigare il rischio di Account Takeover, implementare l'autenticazione a più fattori (MFA) obbligatoria per tutti gli account, o almeno per le operazioni sensibili come il reset della password e l'accesso successivo. Questo aggiunge un ulteriore livello di sicurezza, garantendo che anche se un token di reset viene compromesso, un attaccante non possa completare l'account takeover senza il secondo fattore.

CVSS Metrics

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

CWE - Common Weakness Enumeration

613: **Insufficient Session Expiration**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-26051 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazioni non autorizzate delle stazioni e di 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 stazioni di ricarica, manipolando dati e comandi. Ciò può causare interruzioni del servizio, transazioni fraudolente e la compromissione dell'integrità dei dati operativi.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.10% (Percentile: 0.28) Disponibili 2 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un reverse proxy o un Web Application Firewall (WAF) davanti agli endpoint WebSocket OCPP. Configurare questi dispositivi per imporre un'autenticazione robusta a livello di infrastruttura, come l'autenticazione basata su certificati o token, prima di inoltrare le connessioni al servizio backend. Questo agisce come un meccanismo di controllo degli accessi supplementare per prevenire impersonificazioni non autorizzate delle stazioni.

CVSS Metrics

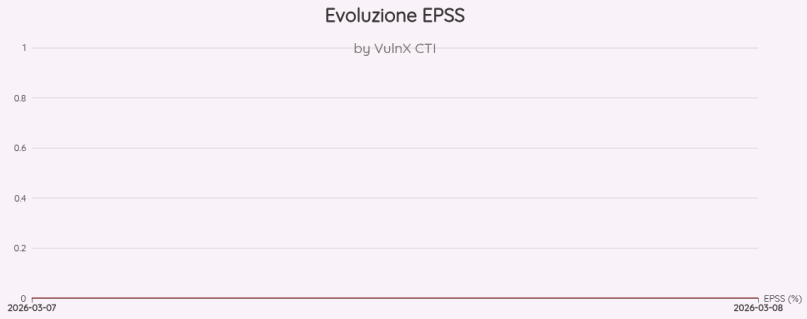
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-26288 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazioni non autorizzate delle stazioni e di manipolare i dati inviati al backend. Un attaccante non autenticato può connettersi all'endpoint WebSocket OCPP utilizzando un identificativo 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?

Gli attaccanti possono impersonare stazioni di ricarica e manipolare i dati e i comandi scambiati, causando interruzioni del servizio e potenziali frodi. Questa vulnerabilità permette un controllo non autorizzato dei sistemi, con conseguenti significative perdite finanziarie e danni alla reputazione aziendale.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.07% (Percentile: 0.22) Disponibili 2 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un API Gateway o un reverse proxy robusto davanti agli endpoint WebSocket OCPP. Questo permetterà di imporre meccanismi di autenticazione forti, come certificati client o mTLS, prima che le connessioni raggiungano l'applicazione backend, compensando così la mancanza di autenticazione intrinseca.

CVSS Metrics

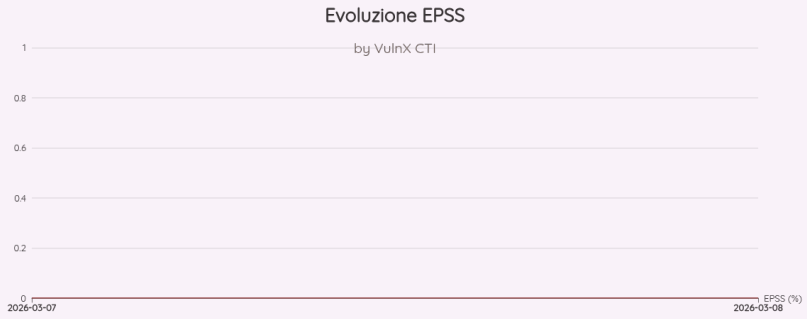
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-2330 - CVSS 9.4 (CRITICA)

Un attaccante potrebbe accedere ad aree del filesystem ristrette sul dispositivo tramite l'interfaccia CROWN REST a causa di un'applicazione incompleta della whitelist. Alcuna directory destinate ai test interni non erano coperte dalla whitelist e sono accessibili senza autenticazione. Un attaccante non autenticato potrebbe posizionare un file di parametri manipolato che diventa attivo dopo un riavvio, consentendo la modifica di impostazioni critiche del dispositivo, inclusa la configurazione di rete e i parametri delle applicazioni.

Descrizione Originale (EN): An attacker may access restricted filesystem areas on the device via the CROWN REST interface due to incomplete whitelist enforcement. Certain directories intended for internal testing were not covered by the whitelist and are accessible without authentication. An unauthenticated attacker could place a manipulated parameter file that becomes active after a reboot, allowing modification of critical device settings, including network configuration and application parameters.

Cosa può succedere?
Un attaccante non autenticato potrebbe alterare le configurazioni critiche del dispositivo, compromettendone il funzionamento e la sicurezza. Ciò potrebbe portare a gravi interruzioni di servizio, manipolazione dei dati o al controllo completo del sistema.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.21% (Percentile: 0.43) Disponibili 3 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolate i dispositivi che espongono l'interfaccia CROWN REST in una zona di rete dedicata e altamente ristretta. Configurate regole firewall per limitare l'accesso a tale interfaccia solo da indirizzi IP o sottoreti strettamente autorizzate, riducendo drasticamente l'esposizione a potenziali attaccanti non autenticati.

CVSS Metrics

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

CWE - Common Weakness Enumeration

552: **Files or Directories Accessible to External Parties**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-22552 - CVSS 9.4 (CRITICA)

Gli endpoint WebSocket mancano di meccanismi di autenticazione adeguati, consentendo agli attaccanti di eseguire impersonificazioni non autorizzate delle stazioni e di 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 potrebbe impersonare una stazione di ricarica legittima, manipolare i dati inviati al backend e inviare comandi non autorizzati. Ciò potrebbe causare interruzioni del servizio, transazioni fraudolente e compromettere gravemente l'integrità dei dati operativi e la sicurezza dell'infrastruttura.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.10% (Percentile: 0.28) Disponibili 3 valori storici
Pubblicata:	06/03/2026
Modificata:	06/03/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare gli endpoint WebSocket OCPP in una zona di rete strettamente segmentata (DMZ). Implementare regole firewall restrittive per consentire l'accesso a questi endpoint solo da indirizzi IP pre-autorizzati e noti delle stazioni di ricarica o del sistema backend, bloccando qualsiasi tentativo di connessione 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:** low

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

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-2017-7921 KEV

CVSS: 10.0/10 **EPSS:** 94.3% **Target:** Unknown **Rischio:** 9.8/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica per il suo punteggio CVSS massimo di 10.0, l'altissima probabilità di sfruttamento (EPSS 94.3%) e il suo stato di vulnerabilità attivamente sfruttata (CISA KEV).

Minaccia #2: CVE-2021-22681 KEV

CVSS: 9.8/10 **EPSS:** 15.4% **Target:** Unknown **Rischio:** 7.3/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché il suo punteggio CVSS di 9.8 indica una gravità estrema e la sua presenza nel CISA KEV conferma lo sfruttamento attivo, consentendo esecuzione di codice remoto non autenticata.

Minaccia #3: CVE-2023-43000 KEV

CVSS: 8.8/10 **EPSS:** 0.1% **Target:** Unknown **Rischio:** 6.3/10

Perché è una minaccia prioritaria:
Questo CVE rappresenta una minaccia critica a causa del suo alto punteggio CVSS (8.8) e, soprattutto, perché è attivamente sfruttato, come confermato dall'inclusione nel 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