VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Settimanale

16/02/2026 - 23/02/2026

Generato il: **23/02/2026 08:15**

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 registrate 1366 nuove CVE, con 79 classificate come critiche e 359 come alte. È di particolare rilevanza la presenza di 8 vulnerabilità aggiunte al CISA KEV e 4 con un punteggio EPSS superiore al 50%, indicando un'alta probabilità di exploit attivo.
Azione Consigliata: Si raccomanda di prioritizzare immediatamente la mitigazione delle 8 CVE presenti nel CISA KEV e delle 4 con EPSS >50%, data la loro elevata probabilità di sfruttamento. È fondamentale inoltre monitorare attentamente le 79 vulnerabilità critiche e le 359 ad alta gravità per applicare le patch non appena disponibili.

Metrica	Valore
Totale CVE	**1366**
Critiche	**79**
Alte	**359**
EPSS >50%	**4**
KEV	**8**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	1,359	–
CVE Modificate	2,161	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	79	7.6%
Alte (7.0-8.9)	359	34.3%
Medie (4.0-6.9)	538	51.4%
Basse (0.1-3.9)	70	6.7%
Indicatori di Rischio		
KEV (Exploit Attivi)	8	0.6%
EPSS Elevato (>50%)	4	0.3%

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

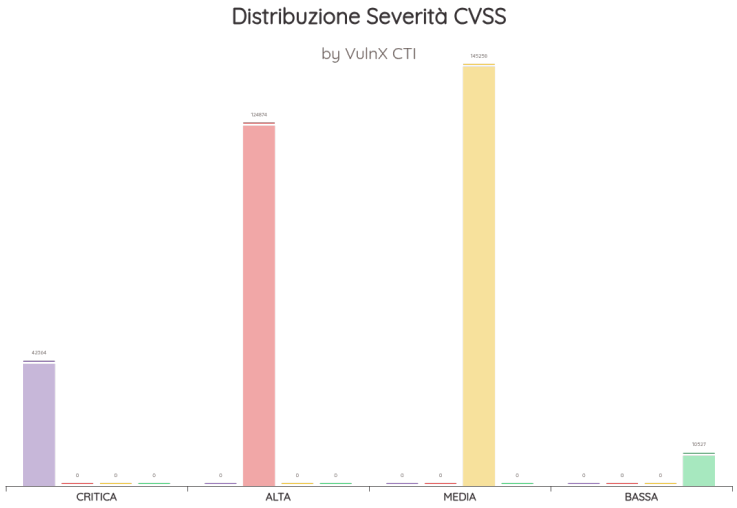
1.2 Panoramica Database (Storico Completo)

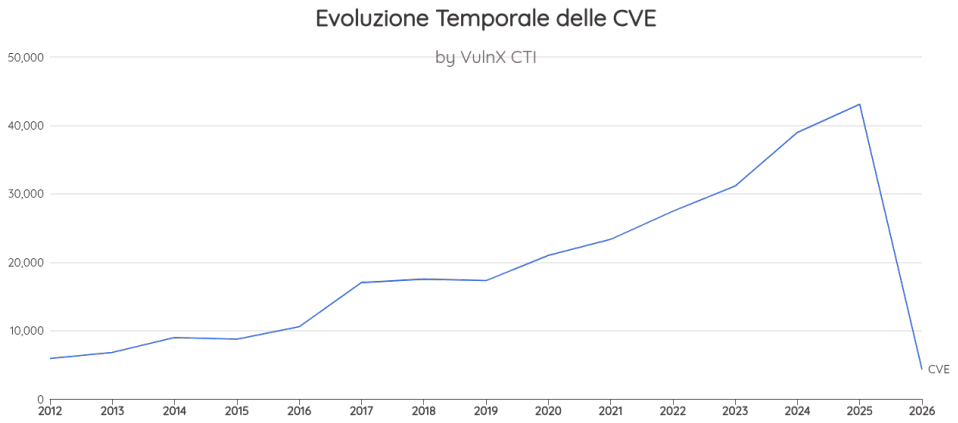
Statistiche complete del database storico su tutte le CVE mai pubblicate:

- **CVE Totali nel Database:** 334,293
- **KEV Totali (Vulnerabilità con Exploit Noti):** 1,528
- **CWE Totali Catalogate:** 969
- **CPE Totali Monitorati:** 2,206,017

Severità	Conteggio	Percentuale
CRITICA	42,364	13.1%
ALTA	124,874	38.7%
MEDIA	145,258	45.0%
BASSA	10,527	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:

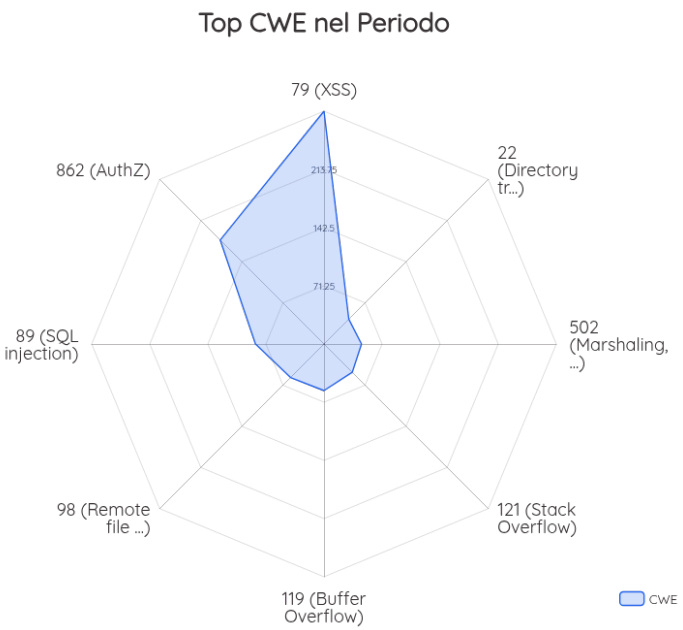


Figura 1: *Distribuzione Top CWE - Grafico Radar*

3.2 Analisi Approfondita delle Debolezze (CWE)

Le debolezze più comuni con raccomandazioni di difesa.

79

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

▶ **Occorrenze:** 285

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per mitigare la CWE-79 (Cross-site Scripting):
- N/A**Codifica dell'Output Contestuale:**Implementare sempre la codifica dell'output (HTML-encoding, URL-encoding, JavaScript-encoding, ecc.) per tutti i dati forniti dall'utente prima di renderizzarli nella pagina web. Utilizzare funzioni di codifica specifiche per il contesto in cui i dati verranno visualizzati.
- N/A**Content Security Policy (CSP):**Configurare una Content Security Policy (CSP) restrittiva tramite l'header HTTP. Questo permette di definire le origini consentite per script, stili e altri contenuti, bloccando l'esecuzione di script iniettati da fonti non autorizzate.
- N/A**Web Application Firewall (WAF):**Utilizzare un Web Application Firewall (WAF) e configurare regole specifiche per rilevare e bloccare proattivamente i tentativi di attacchi XSS a livello di rete, agendo come una prima linea di difesa.

94

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

- **Occorrenze:** 41

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per mitigare la CWE-94:
- N/A**Utilizzare query parametrizzate o prepared statements:**Per tutte le interazioni con il database, separare rigorosamente il codice SQL dai dati di input utente, prevenendo la SQL Injection.
- N/A**Implementare una validazione rigorosa dell'input basata su whitelisting:**Accettare solo caratteri, formati e valori noti come sicuri e previsti per ogni campo di input, rifiutando qualsiasi altro input.
- N/A**Configurare regole WAF (Web Application Firewall):**Impostare regole WAF per rilevare e bloccare pattern comuni associati a tentativi di code injection (es. SQL Injection, OS Command Injection) a livello di rete.

639

Authorization Bypass Through User-Controlled Key

▶ **Occorrenze:** 18

Raccomandazioni di Difesa

▶ Ecco 2-3 raccomandazioni specifiche e attuabili per la debolezza CWE-639:

▶ N/A**Implementare controlli di autorizzazione granulari lato server:**Per ogni richiesta che utilizza una chiave controllata dall'utente (es. ID, token) per accedere a una risorsa, il server deve *sempre* verificare che l'utente autent

285

Improper Authorization

▶ **Occorrenze:** 9

Raccomandazioni di Difesa

▶ Ecco 3 raccomandazioni specifiche e attuabili per mitigare la debolezza CWE-285 - Improper Authorization:

▶ N/A**Implementare un sistema di controllo degli accessi basato sui ruoli (RBAC) e applicare il principio del privilegio minimo**per utenti, servizi e processi, garantendo che ogni entità abbia solo i permessi strettamente necessari per svolgere le proprie funzioni.

▶ N/A**Garantire che tutti i controlli di autorizzazione per l'accesso a risorse o funzionalità sensibili siano eseguiti lato server**, mai esclusivamente lato client, e che siano verificati ad ogni richiesta.

▶ N/A**Utilizzare un'API Gateway o un servizio di autorizzazione dedicato**per centralizzare e applicare le politiche di accesso tra i microservizi o le applicazioni, fornendo un punto di controllo unico e robusto.

1336

Improper Neutralization of Special Elements Used in a Template Engine

▶ **Occorrenze:** 3

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-1336:
- N/A**Pratiche di Sviluppo:**Implementare l'escaping contestuale di tutti i dati forniti dall'utente prima della renderizzazione nei template. Assicurarsi che l'escaping sia appropriato per il contesto di output specifico (HTML, attributo, JavaScript, CSS, ecc.).
- N/A**Configurazioni di Sicurezza:**Configurare i motori di template per disabilitare funzionalità pericolose (es. accesso al filesystem, esecuzione di codice arbitrario) e applicare il principio del privilegio minimo alle capacità dei template.
- N/A**Strumenti di Sicurezza:**Integrare strumenti SAST (Static Application Security Testing) nel pipeline CI/CD per rilevare automaticamente vulnerabilità di iniezione nei template e condurre revisioni del codice mirate sulla gestione dei dati nei template.

940

Improper Verification of Source of a Communication Channel

▶ **Occorrenze:** 2

Raccomandazioni di Difesa

- Ecco 2-3 raccomandazioni specifiche e attuabili per CWE-940:
- N/A**Configurare regole di firewall e Security Group:**Limitare l'accesso ai canali di comunicazione critici o sensibili solo da indirizzi IP o range di rete predefiniti e fidati.
- N/A**Implementare l'autenticazione mutua TLS (mTLS):**Richiedere l'autenticazione reciproca tramite certificati digitali per le comunicazioni tra servizi (server-to-server) e per l'accesso a canali critici, garantendo che entrambe le parti verifichino l'identità dell'altra.
- N/A**Validare l'identità del mittente a livello applicativo:**Per le comunicazioni non protette da mTLS o per i payload, implementare la verifica dell'identità del mittente tramite token (es. JWT), API keys robuste o firme digitali sui messaggi, assicurandosi che siano validi e non manomessi.

3.3 CVE del Periodo Analizzato

Trovate **1359** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **25** CVE:

CVE-2021-35402 - CVSS 10.0 (CRITICA)

PROLiNK PRC2402M 20190909 prima del 2021-06-13 consente l'iniezione di comandi OS tramite live_api.cgi?page=satellite_list mediante metacaratteri shell nel parametro ip (per satellite_status).

Descrizione Originale (EN): PROLiNK PRC2402M 20190909 before 2021-06-13 allows live_api.cgi?page=satellite_list OS command injection via shell metacharacters in the ip parameter (for satellite_status).

Cosa può succedere?
Un attaccante potrebbe ottenere il controllo completo del dispositivo vulnerabile. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi essenziali o all'utilizzo del dispositivo come punto di partenza per attacchi più ampi alla rete aziendale.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.27% (Percentile: 0.50) Disponibili 2 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Per mitigare il rischio critico dato dall'assenza di una patch, isolare il dispositivo PROLiNK PRC2402M implementando una rigorosa segmentazione di rete. Collocarlo in una VLAN dedicata con regole firewall che limitino l'accesso alla sua interfaccia di gestione e alle porte critiche esclusivamente da host e reti interne strettamente necessarie. Questo ridurrà drasticamente la superficie d'attacco.

CVSS Metrics

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

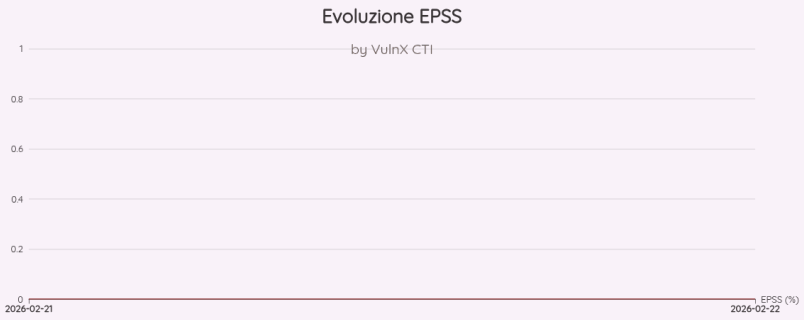
CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

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

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-27574 - CVSS 9.9 (CRITICA)

OneUptime è una soluzione per il monitoraggio e la gestione dei servizi online. Nelle versioni 9.5.13 e precedenti, la funzione di monitoraggio personalizzato con JavaScript utilizza il modulo node:vm di Node.js (esplicitamente documentato come non un meccanismo di sicurezza) per eseguire codice fornito dall'utente, consentendo una facile fuga dal sandbox tramite una nota riga di comando che garantisce l'accesso completo al processo sottostante. Poiché il probe viene eseguito con il networking dell'host e contiene tutte le credenziali del cluster (ONEUPTIME_SECRET, DATABASE_PASSWORD, REDIS_PASSWORD, CLICKHOUSE_PASSWORD) nelle variabili d'ambiente, e la creazione di monitor è disponibile al ruolo più basso (ProjectMember) con l'iscrizione aperta abilitata di default, qualsiasi utente anonimo può ottenere il compromesso completo del cluster in circa 30 secondi. Questo problema è stato risolto nella versione 10.0.5.

Descrizione Originale (EN): OneUptime is a solution for monitoring and managing online services. In versions 9.5.13 and below, custom JavaScript monitor feature uses Node.js's node:vm module (explicitly documented as not a security mechanism) to execute user-supplied code, allowing trivial sandbox escape via a well-known one-liner that grants full access to the underlying process. Because the probe runs with host networking and holds all cluster credentials (ONEUPTIME_SECRET, DATABASE_PASSWORD, REDIS_PASSWORD, CLICKHOUSE_PASSWORD) in its environment variables, and monitor creation is available to the lowest role (ProjectMember) with open registration enabled by default, any anonymous user can achieve full cluster compromise in about 30 seconds. This issue has been fixed in version 10.0.5.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo del server che esegue OneUptime, accedendo a dati sensibili e utilizzandolo come punto di partenza per compromettere l'intera rete aziendale. Ciò potrebbe portare a gravi interruzioni dei servizi, furto di informazioni critiche e danni reputazionali significativi.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.05% (Percentile: 0.15) Disponibili 2 valori storici
Pubblicata:	21/02/2026
Modificata:	21/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Data la gravità della vulnerabilità e l'assenza di una patch, isolare immediatamente l'istanza di OneUptime in una rete segmentata e dedicata. Questo ridurrà significativamente la superficie d'attacco e limiterà il movimento laterale di un eventuale aggressore, impedendo l'accesso a risorse interne critiche anche in caso di fuga dalla sandbox. Applicare rigorose regole di firewall per consentire solo le comunicazioni strettamente necessarie da e verso l'istanza.

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

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-2026-24494 - CVSS 9.8 (CRITICA)

Vulnerabilità di SQL Injection nell'endpoint /api/integrations/getintegrations del Order Up Online Ordering System 1.0 consente a un attaccante non autenticato di accedere a dati sensibili del database backend tramite un parametro store_id manipolato in una richiesta POST.

Descrizione Originale (EN): SQL Injection vulnerability in the /api/integrations/getintegrations endpoint of Order Up Online Ordering System 1.0 allows an unauthenticated attacker to access sensitive backend database data via a crafted store_id parameter in a POST request.

Cosa può succedere?

Un attaccante non autenticato potrebbe rubare dati sensibili dal database, come informazioni su clienti e ordini, causando gravi violazioni della privacy. Ciò comporterebbe multe normative, perdita di fiducia dei clienti e un danno reputazionale significativo per l'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	23/02/2026
Modificata:	23/02/2026
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 monte dell'applicazione Order Up Online Ordering System. Configurare il WAF per ispezionare e filtrare il traffico in entrata, bloccando attivamente pattern di SQL Injection e tentativi di manipolazione del parametro 'store_id' prima che raggiungano l'endpoint vulnerabile. Questo aggiunge un livello di protezione critico contro attacchi noti, fungendo da controllo 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

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-2026-2635 - CVSS 9.8 (CRITICA)

Vulnerabilità di bypass dell'autenticazione tramite password predefinita in MLflow. Questa vulnerabilità consente agli attaccanti remoti di bypassare l'autenticazione sugli ambienti MLflow interessati. Non è richiesta l'autenticazione per sfruttare questa vulnerabilità. Il difetto specifico risiede nel file basic_auth.ini. Il file contiene credenziali predefinite hard-coded. Un attaccante può sfruttare questa vulnerabilità per bypassare l'autenticazione ed eseguire codice arbitrario nel contesto dell'amministratore. Era ZDI-CAN-28256.

Descrizione Originale (EN): MLflow Use of Default Password Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of MLflow. Authentication is not required to exploit this vulnerability. The specific flaw exists within the basic_auth.ini file. The file contains hard-coded default credentials. An attacker can leverage this vulnerability to bypass authentication and execute arbitrary code in the context of the administrator. Was ZDI-CAN-28256.

Cosa può succedere?
Un attaccante remoto può ottenere il pieno controllo degli ambienti MLflow, accedendo a dati sensibili e modelli di machine learning. Questo permette il furto di informazioni critiche, la manipolazione dei sistemi o la compromissione dell'intera infrastruttura IT aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	1.17% (Percentile: 0.78) Disponibili 2 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare una rigorosa segmentazione della rete per limitare l'accesso all'istanza MLflow. Assicurarsi che l'accesso sia consentito solo da indirizzi IP o subnet interne affidabili e autorizzate, riducendo drasticamente la superficie di attacco esposta a internet o a reti non fidate.

CVSS Metrics

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

CWE - Common Weakness Enumeration

1393: **Use of Default Password**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2019-25441 - CVSS 9.8 (CRITICA)

thesystem 1.0 contiene una vulnerabilità di command injection che consente agli attori malevoli non autenticati di eseguire comandi di sistema arbitrari inviando input dannoso all'endpoint run_command. Gli attori malevoli possono inviare richieste POST con comandi shell nel parametro command per eseguire codice arbitrario sul server senza autenticazione.

Descrizione Originale (EN): thesystem 1.0 contains a command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious input to the run_command endpoint. Attackers can send POST requests with shell commands in the command parameter to execute arbitrary code on the server without authentication.

Cosa può succedere?

Sfruttando questa vulnerabilità, attaccanti non autenticati possono ottenere il controllo completo del server, permettendo il furto di dati sensibili, l'interruzione dei servizi critici o l'installazione di software malevolo. Ciò può portare a gravi perdite finanziarie e danni reputazionali per l'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	2.65% (Percentile: 0.85) Disponibili 2 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
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) davanti a "thesystem 1.0". Configurare il WAF per ispezionare e filtrare attivamente le richieste dirette all'endpoint 'run_command', bloccando specificamente i pattern di command injection noti nel parametro 'command' per prevenire l'esecuzione di codice arbitrario da parte di attori 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

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

Probabilità di Sfruttamento: high

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25715 - CVSS 9.8 (CRITICA)

L'interfaccia di gestione web del dispositivo consente di impostare username e password dell'amministratore su valori vuoti. Una volta applicata, il dispositivo permette l'autenticazione con credenziali vuote attraverso l'interfaccia di gestione web e il servizio Telnet. Ciò disabilita efficacemente l'autenticazione su tutti i canali di gestione critici, consentendo a qualsiasi attaccante adiacente alla rete di ottenere il controllo amministrativo completo senza credenziali.

Descrizione Originale (EN): The web management interface of the device allows the administrator username and password to be set to blank values. Once applied, the device permits authentication with empty credentials over the web management interface and Telnet service. This effectively disables authentication across all critical management channels, allowing any network-adjacent attacker to gain full administrative control without credentials.

Cosa può succedere?

Un attaccante adiacente alla rete può ottenere il controllo amministrativo completo dei dispositivi senza credenziali. Ciò comporta interruzioni critiche dei servizi, furto di dati sensibili e la potenziale compromissione dell'intera rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.06% (Percentile: 0.18) Disponibili 2 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
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 dispositivo in una VLAN di gestione dedicata e non instradabile dalla rete principale. Applicare regole firewall per consentire l'accesso alle interfacce di gestione (web, Telnet) solo da workstation amministrative autorizzate e indirizzi IP specifici, bloccando ogni altro tentativo di connessione.

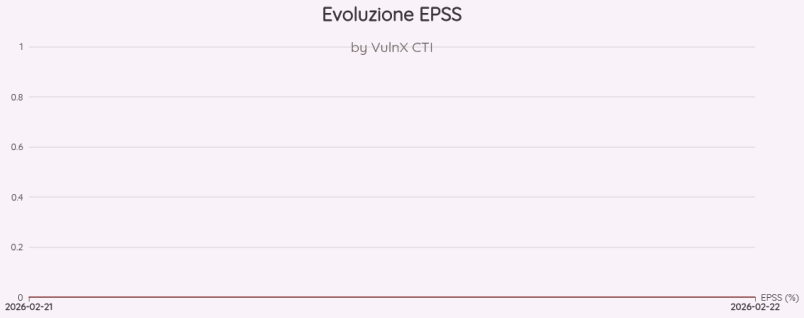
CVSS Metrics

- **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

521: **Weak Password Requirements**

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2025-10970 - CVSS 9.8 (CRITICA)

Impropia neutralizzazione di elementi speciali utilizzati in un comando SQL ('SQL Injection') vulnerabilità in Kolay Software Inc. Talentics consente l'SQL Injection cieco. Questo problema riguarda Talentics: attraverso 20022026. 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 Kolay Software Inc. Talentics allows Blind SQL Injection.This issue affects Talentics: through 20022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?

Gli attaccanti potrebbero ottenere accesso non autorizzato al database, rubando dati sensibili come informazioni personali dei dipendenti, dati finanziari o segreti aziendali. Tale accesso potrebbe anche consentire la manipolazione dei dati e l'interruzione dei servizi aziendali critici.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.03% (Percentile: 0.09) Disponibili 3 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
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) a protezione dell'applicazione Talentics, configurandolo per rilevare e bloccare attivamente tentativi di SQL Injection. Questo controllerà e filtrerà il traffico HTTP/S in ingresso, prevenendo che input malevoli raggiungano l'applicazione e sfruttino la vulnerabilità di iniezione SQL cieca.

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-2026-21627 - CVSS 9.5 (CRITICA)

La vulnerabilità era radicata nel modo in cui il plugin Tassos Framework gestiva specifiche richieste AJAX tramite il punto di ingresso com_ajax di Joomla. In determinate condizioni, la funzionalità interna del framework poteva essere richiamata senza le dovute restrizioni.

Descrizione Originale (EN): The vulnerability was rooted in how the Tassos Framework plugin handled specific AJAX requests through Joomla's com_ajax entry point. Under certain conditions, internal framework functionality could be invoked without proper restriction.

Cosa può succedere?

Sfruttando questa vulnerabilità, un attaccante può ottenere il pieno controllo del server web. Ciò permette il furto di dati sensibili, l'interruzione dei servizi online e la potenziale compromissione di altri sistemi aziendali.

Punteggio CVSS:	9.5 (CRITICA)
EPSS:	0.01% (Percentile: 0.02) Disponibili 2 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Data l'assenza di una patch e la gravità della vulnerabilità, implementare un Web Application Firewall (WAF) a protezione dell'istanza Joomla è una misura infrastrutturale critica. Configurare il WAF per monitorare e bloccare proattivamente le richieste anomale dirette all'endpoint 'com_ajax', specialmente quelle che tentano di abusare delle funzionalità del plugin Tassos Framework, può mitigare significativamente l'esposizione.

CVSS Metrics

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

CWE - Common Weakness Enumeration

284: **Improper Access Control**

Termini Alternativi: Authorization

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27212 - CVSS 9.4 (CRITICA)

Swiper è un componente slider touch gratuito e mobile con transizioni accelerate dall'hardware e comportamento nativo. Le versioni dalla 6.5.1 alla 12.1.1 presentano una vulnerabilità di Prototype pollution. La vulnerabilità risiede nella riga 94 di shared/utils.mjs, dove la funzione indexOf() viene utilizzata per verificare se l'input fornito dall'utente contiene stringhe proibite. Nonostante una precedente patch che tentava di mitigare il prototype pollution controllando se l'input dell'utente contenesse una chiave proibita, è ancora possibile inquinare Object.prototype tramite un input manipolato utilizzando Array.prototype. L'exploit funziona su Windows e Linux e sui runtime Node e Bun. Qualsiasi applicazione che processa input controllato dall'attaccante utilizzando questo pacchetto potrebbe essere soggetta a: Bypass dell'autenticazione, Denial of Service e RCE. Il problema è stato risolto nella versione 12.1.2.

Descrizione Originale (EN): Swiper is a free and mobile touch slider with hardware accelerated transitions and native behavior. Versions 6.5.1 through 12.1.1 have a Prototype pollution vulnerability. The vulnerability resides in line 94 of shared/utils.mjs, where the indexOf() function is used to check whether user provided input contain forbidden strings. Despite a previous fix that attempted to mitigate prototype pollution by checking whether user input contained a forbidden key, it is still possible to pollute Object.prototype via a crafted input using Array.prototype. The exploit works across Windows and Linux and on Node and Bun runtimes. Any application that processes attacker-controlled input using this package may be affected by the following: Authentication Bypass, Denial of Service and RCE. This issue is fixed in version 12.1.2.

Cosa può succedere?

L'exploit di questa vulnerabilità può consentire a un attaccante di prendere il controllo dei sistemi che utilizzano Swiper. Ciò potrebbe portare al furto di dati sensibili, alla manipolazione delle informazioni aziendali o a una grave interruzione dei servizi.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.03% (Percentile: 0.09) Disponibili 2 valori storici
Pubblicata:	21/02/2026
Modificata:	21/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Considerate l'implementazione o il rafforzamento di una Web Application Firewall (WAF) per monitorare e filtrare attivamente il traffico in ingresso. Configurate il WAF per rilevare e bloccare pattern di input malevoli che potrebbero tentare di sfruttare vulnerabilità client-side come la prototype pollution, intercettandoli prima che raggiungano l'applicazione.

CVSS Metrics

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

CWE - Common Weakness Enumeration

1321: **Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')**

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27112 - CVSS 9.4 (CRITICA)

Kargo gestisce e automatizza la promozione degli artefatti software. Dalla versione 1.7.0 fino alle versioni precedenti a v1.7.8, v1.8.11 e v1.9.3, gli endpoint di creazione batch delle risorse sia dell'API legacy gRPC di Kargo sia della più recente API REST accettano payload YAML multi-documento. Payload appositamente costruiti possono manifestare un bug presente nella logica di entrambi gli endpoint, consentendo l'iniezione di risorse arbitrarie (di tipi specifici) nel namespace sottostante di un progetto esistente utilizzando i permessi del server API, quando tale comportamento non era previsto. Criticamente, un attaccante può sfruttare questa vulnerabilità come vettore per elevare i propri permessi, che possono poi essere utilizzati per eseguire codice remoto o esfiltrare secret. Le credenziali dell'artefatto repository esfiltrate possono essere a loro volta utilizzate per attacchi successivi. In alcune configurazioni del control plane di Kargo e del cluster Kubernetes sottostante, i permessi elevati possono essere ulteriormente sfruttati per eseguire codice remoto o esfiltrare secret tramite kubectl. Questo può ridurre la complessità dell'attacco; tuttavia, scenari peggiori sono comunque pienamente realizzabili anche senza questa vulnerabilità. Questa vulnerabilità è stata corretta nelle versioni v1.7.8, v1.8.11 e v1.9.3.

Descrizione Originale (EN): Kargo manages and automates the promotion of software artifacts. From 1.7.0 to before v1.7.8, v1.8.11, and v1.9.3, the batch resource creation endpoints of both Kargo's legacy gRPC API and newer REST API accept multi-document YAML payloads. Specially crafted payloads can manifest a bug present in the logic of both endpoints to inject arbitrary resources (of specific types only) into the underlying namespace of an existing Project using the API server's own permissions when that behavior was not intended. Critically, an attacker may exploit this as a vector for elevating their own permissions, which can then be leveraged to achieve remote code execution or secret exfiltration. Exfiltrated artifact repository credentials can be leveraged, in turn, to execute further attacks. In some configurations of the Kargo control plane's underlying Kubernetes cluster, elevated permissions may additionally be leveraged to achieve remote code execution or secret exfiltration using kubectl. This can reduce the complexity of the attack, however, worst case scenarios remain entirely achievable even without this. This vulnerability is fixed in v1.7.8, v1.8.11, and v1.9.3.

Cosa può succedere?

Sfruttando questa vulnerabilità, un attaccante potrebbe iniettare risorse malevole per ottenere il controllo non autorizzato su parti critiche del sistema. Ciò potrebbe causare gravi interruzioni del servizio, manipolazione dei dati e la compromissione dell'infrastruttura sottostante, con impatto diretto sulle operazioni aziendali.

Punteggio CVSS:	9.4 (CRITICA)
EPSS:	0.24% (Percentile: 0.47) Disponibili 2 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementate un Web Application Firewall (WAF) o un API Gateway davanti agli endpoint API di Kargo. Configurate queste soluzioni per ispezionare e filtrare rigorosamente i payload YAML in ingresso, bloccando specificamente i payload multi-documento o quelli che non rispettano una whitelist di strutture valide, prevenendo così lo sfruttamento della vulnerabilità.

CVSS Metrics

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

CWE - Common Weakness Enumeration

863: **Incorrect Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27471 - CVSS 9.3 (CRITICA)

ERP è uno strumento di Enterprise Resource Planning gratuito e open source. Nelle versioni fino alla 15.98.0 e alla 16.0.0-rc.1 e fino alla 16.6.0, alcuni endpoint mancavano di validazione degli accessi, consentendo l'accesso non autorizzato ai documenti. Questo problema è stato risolto nelle versioni 15.98.1 e 16.6.1.

Descrizione Originale (EN): ERP is a free and open source Enterprise Resource Planning tool. In versions up to 15.98.0 and 16.0.0-rc.1 and through 16.6.0, certain endpoints lacked access validation which allowed for unauthorized document access. This issue has been fixed in versions 15.98.1 and 16.6.1.

Cosa può succedere?

Un aggressore potrebbe accedere senza autorizzazione a documenti aziendali sensibili all'interno del sistema ERP. Ciò comporta il rischio di furto di dati critici (finanziari, clienti, strategici), gravi violazioni della privacy, danni reputazionali e potenziali sanzioni normative.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 2 valori storici
Pubblicata:	21/02/2026
Modificata:	21/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) o un API Gateway davanti al sistema ERP per filtrare e bloccare attivamente i tentativi di accesso non autorizzato agli endpoint vulnerabili. Configurare regole di sicurezza stringenti per monitorare e prevenire l'accesso illecito ai documenti, agendo come controllo compensativo critico.

CVSS Metrics

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

CWE - Common Weakness Enumeration

284: **Improper Access Control**

Termini Alternativi: Authorization

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

862: **Missing Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25896 - CVSS 9.3 (CRITICA)

fast-xml-parser consente agli utenti di convalidare XML, analizzare XML in oggetto JS o costruire XML da oggetto JS senza librerie basate su C/C++ e senza callback. Dalla versione 4.1.3 fino alla precedente alla 5.3.5, un punto (.) nel nome di un'entità DOCTYPE viene trattato come un carattere jolly regex durante la sostituzione delle entità, consentendo a un attaccante di sovrascrivere le entità XML integrate (<, >, &, ", ') con valori arbitrari. Ciò bypassa la codifica delle entità e può portare a XSS quando l'output analizzato viene renderizzato. Questa vulnerabilità è stata corretta in versione 5.3.5.

Descrizione Originale (EN): fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. From 4.1.3to before 5.3.5, a dot (.) in a DOCTYPE entity name is treated as a regex wildcard during entity replacement, allowing an attacker to shadow built-in XML entities (<, >, &, ", ') with arbitrary values. This bypasses entity encoding and leads to XSS when parsed output is rendered. This vulnerability is fixed in 5.3.5.

Cosa può succedere?

Un attaccante potrebbe iniettare codice malevolo o manipolare i dati XML, compromettendo la riservatezza e l'integrità delle informazioni aziendali. Ciò potrebbe causare il furto di dati sensibili, interruzioni dei servizi critici o il controllo non autorizzato dei sistemi.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.03% (Percentile: 0.08) Disponibili 2 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
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) a livello di infrastruttura per ispezionare e filtrare il traffico XML in ingresso. Configurare il WAF per rilevare e bloccare pattern di attacco noti, inclusi tentativi di manipolazione delle entità DOCTYPE, che potrebbero sfruttare questa vulnerabilità. Questo servirà come controllo compensativo per proteggere le applicazioni che utilizzano 'fast-xml-parser'.

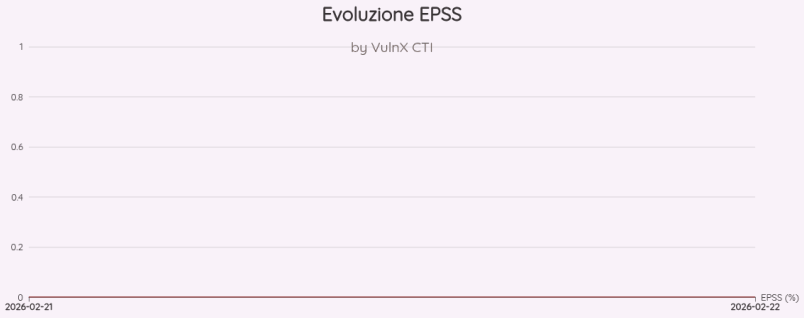
CVSS Metrics

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

CWE - Common Weakness Enumeration

185: **Incorrect Regular Expression**

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-27452 - CVSS 9.2 (CRITICA)

Libreria ASN.1 TypeScript ESM, inclusi codec per le Basic Encoding Rules (BER) e le Distinguished Encoding Rules (DER). Nelle versioni 11.0.5 e precedenti, in alcuni casi, il decoding di un INTEGER potrebbe rivelare l'ArrayBuffer sottostante. Si prevede che questo problema venga risolto nella versione 11.0.6.

Descrizione Originale (EN): ASN.1 TypeScript ESM library, including codecs for Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER). In versions 11.0.5 and below, in some cases, decoding an INTEGER could leak the underlying ArrayBuffer. This issue is expected to be fixed in version 11.0.6.

Cosa può succedere?

Sfruttando questa vulnerabilità, un aggressore potrebbe accedere a dati sensibili in memoria, come chiavi crittografiche o informazioni personali. Ciò potrebbe causare gravi violazioni dei dati, con conseguenti perdite finanziarie, danni reputazionali e potenziali interruzioni dei servizi aziendali.

Punteggio CVSS:	9.2 (CRITICA)
EPSS:	0.04% (Percentile: 0.13) Disponibili 2 valori storici
Pubblicata:	21/02/2026
Modificata:	21/02/2026
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 avanzato per le applicazioni che utilizzano la libreria ASN.1 TypeScript vulnerabile. Focalizzarsi sulla rilevazione di accessi anomali alla memoria, traffico di rete in uscita inatteso o attività di elaborazione dati sospette che potrebbero indicare lo sfruttamento della vulnerabilità di esposizione dell'ArrayBuffer. Questo aiuterà a identificare e mitigare rapidamente potenziali esfiltrazioni di dati o compromissioni.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Termini Alternativi: Information Disclosure, Information Leak

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-2333 - CVSS 9.2 (CRITICA)

Neutralizzazione impropria di elementi speciali utilizzati in un comando ('Command Injection') in Owl opds 2.2.0.4 consente l'iniezione di comandi tramite una richiesta di rete appositamente manipolata.

Descrizione Originale (EN): Improper Neutralization of Special Elements used in a Command ('Command Injection') in Owl opds 2.2.0.4 allows Command Injection via a crafted network request.

Cosa può succedere?

Un attaccante potrebbe ottenere il pieno controllo dei sistemi interessati, consentendo il furto di dati sensibili, l'interruzione dei servizi critici o l'installazione di software malevolo. Questo potrebbe causare gravi perdite finanziarie e danni reputazionali per l'azienda.

Punteggio CVSS:	9.2 (CRITICA)
EPSS:	0.59% (Percentile: 0.69) Disponibili 2 valori storici
Pubblicata:	20/02/2026
Modificata:	20/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare una rigorosa segmentazione della rete e regole firewall per limitare l'accesso diretto all'istanza Owl opds 2.2.0.4 da reti non attendibili o da Internet. Consentire la connettività solo da sistemi interni fidati strettamente necessari e, se possibile, tramite jump host dedicati e induriti. Questo ridurrà significativamente la superficie di attacco e la probabilità di sfruttamento della vulnerabilità.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Termini Alternativi: Command injection

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27211 - CVSS 9.1 (CRITICA)

Cloud Hypervisor è un Virtual Machine Monitor per carichi di lavoro Cloud. Le versioni dalla 34.0 alla 50.0 sono vulnerabili a un'esfiltrazione arbitraria di file host (limitata dai privilegi del processo) quando si utilizzano dispositivi virtio-block supportati da immagini raw. Un guest malintenzionato può sovrascrivere l'intestazione del proprio disco con una struttura QCOW2 appositamente creata, puntando a un percorso sensibile dell'host. Al successivo avvio della VM o scansione del disco, il rilevamento automatico del formato dell'immagine analizza questa intestazione e fornisce i contenuti del file host al guest. Riavvii della VM iniziati dal guest sono sufficienti per attivare una scansione del disco e non causano l'uscita del processo Cloud Hypervisor. Pertanto, un singolo VM può eseguire questo attacco senza bisogno di interazione da parte dello stack di gestione. L'exploit riuscito richiede che l'immagine di supporto sia scrivibile dal guest o proveniente da una fonte non affidabile. Le implementazioni che utilizzano esclusivamente immagini affidabili in sola lettura non sono interessate. Questo problema è stato risolto nella versione 50.1. Per mitigare, si consiglia di abilitare il sandboxing land lock e di limitare i privilegi e gli accessi del processo.

Descrizione Originale (EN): Cloud Hypervisor is a Virtual Machine Monitor for Cloud workloads. Versions 34.0 through 50.0 arevulnerable to arbitrary host file exfiltration (constrained by process privileges) when using virtio-block devices backed by raw images. A malicious guest can overwrite its disk header with a crafted QCOW2 structure pointing to a sensitive host path. Upon the next VM boot or disk scan, the image format auto-detection parses this header and serves the host file's contents to the guest. Guest-initiated VM reboots are sufficient to trigger a disk scan and do not cause the Cloud Hypervisor process to exit. Therefore, a single VM can perform this attack without needing interaction from the management stack. Successful exploitation requires the backing image to be either writable by the guest or sourced from an untrusted origin. Deployments utilizing only trusted, read-only images are not affected. This issue has been fixed in version 50.1. To workaround, enable land lock sandboxing and restrict process privileges and access.

Cosa può succedere?

Un attaccante può rubare file sensibili direttamente dal sistema host, compromettendo la riservatezza dei dati aziendali come credenziali o configurazioni critiche. Ciò può portare a gravi violazioni della sicurezza, perdita di dati e potenziali interruzioni dei servizi.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	0.05% (Percentile: 0.16) Disponibili 2 valori storici
Pubblicata:	21/02/2026
Modificata:	21/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare rigorosi controlli di accesso basati sul principio del minimo privilegio per il processo Cloud Hypervisor. Questo ridurrà significativamente la portata dell'esfiltrazione di file arbitrari dall'host, limitando i dati a cui un attaccante potrebbe accedere anche in caso di sfruttamento della vulnerabilità.

CVSS Metrics

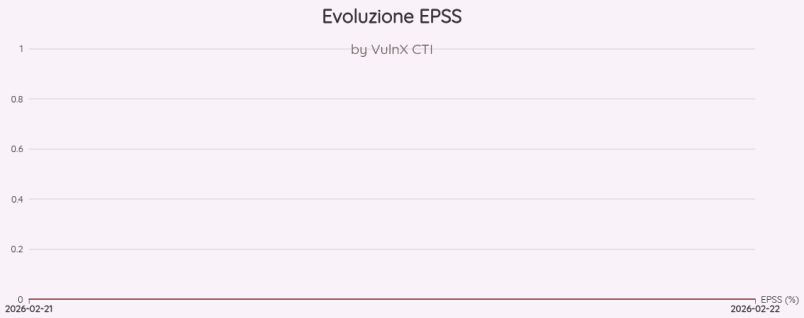
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none

CWE - Common Weakness Enumeration

73: **External Control of File Name or Path**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-27197 - CVSS 9.1 (CRITICA)

Sentry è uno strumento di error tracking e performance monitoring orientato agli sviluppatori. Le versioni dalla 21.12.0 alla 26.1.0 presentano una vulnerabilità critica nell'implementazione di SAML SSO che consente a un attaccante di prendere il controllo di qualsiasi account utente utilizzando un Identity Provider SAML malevolo e un'altra organizzazione sulla stessa istanza di Sentry. Gli utenti self-hosted sono a rischio solo se vengono soddisfatti i seguenti criteri: più di un'organizzazione è configurata (SENTRY_SINGLE_ORGANIZATION = True), oppure un utente malevolo ha accesso e permessi esistenti per modificare le impostazioni SSO di un'altra organizzazione in un'istanza multi-organizzazione. Questo problema è stato risolto nella versione 26.2.0. Per mitigare questa vulnerabilità, si consiglia di implementare l'autenticazione a due fattori basata sull'account utente per impedire a un attaccante di completare l'autenticazione con l'account di una vittima. Gli amministratori dell'organizzazione non possono farlo per conto di un utente; è necessario che gli utenti stessi assicurino che la 2FA sia abilitata sul proprio account.

Descrizione Originale (EN): Sentry is a developer-first error tracking and performance monitoring tool. Versions 21.12.0 through 26.1.0 have a critical vulnerability in its SAML SSO implementation which allows an attacker to take over any user account by using a malicious SAML Identity Provider and another organization on the same Sentry instance. Self-hosted users are only at risk if the following criteria is met: ore than one organizations are configured (SENTRY_SINGLE_ORGANIZATION = True), or malicious user has existing access and permissions to modify SSO settings for another organization in a multo-organization instance. This issue has been fixed in version 26.2.0. To workaround this issue, implement user account-based two-factor authentication to prevent an attacker from being able to complete authentication with a victim's user account. Organization administrators cannot do this on a user's behalf, this requires individual users to ensure 2FA has been enabled for their account.

Cosa può succedere?

Un attaccante potrebbe prendere il controllo di qualsiasi account utente Sentry, accedendo a dati sensibili, codici sorgente e informazioni di monitoraggio. Questo potrebbe portare a furto di dati, interruzione dei servizi di sviluppo e operativi, e potenziale compromissione di altri sistemi aziendali.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 2 valori storici
Pubblicata:	21/02/2026
Modificata:	21/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Data l'assenza di una patch, valutare immediatamente la segregazione dell'istanza Sentry in una rete isolata, limitando l'accesso esterno solo alle fonti strettamente autorizzate. Se l'ambiente è multi-tenant, considerare la migrazione delle organizzazioni più critiche a istanze Sentry dedicate per mitigare il rischio di compromissione incrociata. È inoltre fondamentale rivedere e restringere rigorosamente le configurazioni degli Identity Provider SAML accettati, consentendo solo quelli di comprovata fiducia.

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:** none

CWE - Common Weakness Enumeration

287: **Improper Authentication**

Probabilità di Sfruttamento: high

Termini Alternativi: authentification, AuthN, AuthC

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-27169 - CVSS 8.9 (ALTA)

OpenSift è uno strumento di studio basato su AI che analizza grandi dataset utilizzando ricerca semantica e AI generativa. Le versioni 1.1.2-alpha e inferiori rendono contenuti non affidabili di utenti/modelli nelle superfici dell'interfaccia utente dello strumento di chat utilizzando schemi di interpolazione HTML non sicuri, portando a vulnerabilità XSS. I contenuti memorizzati possono eseguire JavaScript quando visualizzati successivamente in sessioni autenticata. Un attaccante che può influenzare i contenuti memorizzati di studi/quiz/flashcard potrebbe innescare l'esecuzione di script nel browser della vittima, potenzialmente eseguendo azioni come quell'utente nella sessione locale dell'app. Questo problema è stato risolto nella versione 1.1.3-alpha.

Descrizione Originale (EN): OpenSift is an AI study tool that sifts through large datasets using semantic search and generative AI. Versions 1.1.2-alpha and below render untrusted user/model content in chat tool UI surfaces using unsafe HTML interpolation patterns, leading to XSS. Stored content can execute JavaScript when later viewed in authenticated sessions. An attacker who can influence stored study/quiz/flashcard content could trigger script execution in a victim's browser, potentially performing actions as that user in the local app session. This issue has been fixed in version 1.1.3-alpha.

Cosa può succedere?

Un attaccante potrebbe rubare le credenziali degli utenti o i dati sensibili visualizzati, compromettendo la riservatezza delle informazioni. Questo potrebbe portare al furto di account, alla manipolazione dei dati o all'esecuzione di azioni non autorizzate all'interno della piattaforma, con gravi ripercussioni operative e sulla reputazione aziendale.

Punteggio CVSS:	8.9 (ALTA)
EPSS:	0.04% (Percentile: 0.14) Disponibili 2 valori storici
Pubblicata:	21/02/2026
Modificata:	21/02/2026
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 XSS, implementare un Web Application Firewall (WAF) davanti all'applicazione OpenSift. Configurare il WAF per ispezionare e sanificare attivamente gli input degli utenti, bloccando i tentativi di iniezione di codice malevolo (XSS) prima che i dati vengano memorizzati o elaborati dall'applicazione. Ciò fornirà un

CVSS Metrics

- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** low
- **Interazione Utente:** required
- **Ambito:** changed
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** low

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

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

116: **Improper Encoding or Escaping of Output**

Probabilità di Sfruttamento: high

Termini Alternativi: Output Sanitization, Output Validation, Output Encoding

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-2961 - CVSS 8.8 (ALTA)

È stata scoperta una vulnerabilità nel D-Link DWR-M960 1.01.07. Questa interessa la funzione sub_4196C4 del file /boafrm/formVpnConfigSetup del componente VPN Configuration Endpoint. La manipolazione dell'argomento submit-url porta a un overflow del buffer 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 has been found in D-Link DWR-M960 1.01.07. This affects the function sub_4196C4 of the file /boafrm/formVpnConfigSetup of the component VPN Configuration Endpoint. The manipulation of the argument submit-url leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo del router D-Link interessato da remoto. Ciò potrebbe portare all'intercettazione di dati aziendali sensibili, all'interruzione dei servizi di rete o all'accesso non autorizzato alla rete interna dell'azienda.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	23/02/2026
Modificata:	23/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Data la vulnerabilità critica e l'assenza di patch, implementare rigorosi controlli di accesso è fondamentale. Limitare l'accesso all'interfaccia di amministrazione web del D-Link DWR-M960 (in particolare all'endpoint '/boafrm/formVpnConfigSetup') tramite regole firewall. Consentire l'accesso a tale interfaccia solo da indirizzi IP interni o da reti di gestione fidate, bloccando ogni tentativo di accesso remoto non autorizzato da Internet.

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 Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-2960 - CVSS 8.8 (ALTA)

È stata individuata una vulnerabilità in D-Link DWR-M960 1.01.07. La funzione interessata da questo problema è sub_468D64 del file /boafrm/formDhcpv6s. La manipolazione dell'argomento submit-url può portare a un overflow del buffer basato su stack. L'attacco può essere eseguito da remoto. L'exploit è stato pubblicato e può essere utilizzato.

Descrizione Originale (EN): A flaw has been found in D-Link DWR-M960 1.01.07. Affected by this issue is the function sub_468D64 of the file /boafrm/formDhcpv6s. Executing a manipulation of the argument submit-url can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.

Cosa può succedere?

Un attaccante potrebbe ottenere il pieno controllo del router D-Link interessato da remoto. Questo permetterebbe la compromissione della rete, il furto di dati sensibili, il monitoraggio del traffico interno o l'interruzione dei servizi internet critici per le operazioni aziendali.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	23/02/2026
Modificata:	23/02/2026
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 dispositivi D-Link DWR-M960 in una rete segmentata o VLAN dedicata. Implementare rigorose regole firewall per limitare l'accesso all'interfaccia di gestione del dispositivo solo da indirizzi IP o sottoreti fidate e strettamente necessarie, bloccando qualsiasi accesso da Internet o da segmenti non autorizzati.

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 Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-2962 - CVSS 8.8 (ALTA)

È stata individuata una vulnerabilità in D-Link DWR-M960 1.01.07. Questa vulnerabilità interessa la funzione sub_460F30 del file /boafrm/formDateReboot del componente Scheduled Reboot Configuration Endpoint. La manipolazione dell'argomento submit-url 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 D-Link DWR-M960 1.01.07. This vulnerability affects the function sub_460F30 of the file /boafrm/formDateReboot of the component Scheduled Reboot Configuration Endpoint. The manipulation of the argument submit-url results in stack-based buffer overflow. The attack may be performed from remote. The exploit has been made public and could be used.

Cosa può succedere?

Un attaccante remoto potrebbe ottenere il controllo completo del dispositivo D-Link, compromettendo la sicurezza della rete aziendale. Ciò potrebbe portare all'intercettazione del traffico, all'accesso non autorizzato a risorse interne o al furto di dati sensibili.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	23/02/2026
Modificata:	23/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare il rischio di sfruttamento remoto, è fondamentale isolare l'interfaccia di amministrazione del D-Link DWR-M960. Implementare la segmentazione di rete posizionando il dispositivo su una VLAN dedicata, limitando l'accesso a tale segmento solo da host amministrativi autorizzati e interni, impedendo così attacchi diretti da reti non fidate.

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 Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-2959 - CVSS 8.8 (ALTA)

Una vulnerabilità è stata rilevata in D-Link DWR-M960 1.01.07. Affected by this vulnerability is the function sub_44E0F8 del file /boafrm/formNewSchedule. La manipolazione dell'argomento url provoca un overflow del buffer basato su stack. È possibile un'esecuzione remota dell'attacco. L'exploit è ora pubblico e può essere utilizzato.

Descrizione Originale (EN): A vulnerability was detected in D-Link DWR-M960 1.01.07. Affected by this vulnerability is the function sub_44E0F8 of the file /boafrm/formNewSchedule. Performing a manipulation of the argument url results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo dei dispositivi D-Link interessati da remoto. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi di rete essenziali e all'accesso non autorizzato all'intera rete aziendale.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	23/02/2026
Modificata:	23/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Considerando l'esecuzione di codice remota e l'exploit pubblico senza patch, isolare immediatamente il router D-Link DWR-M960 interessato in un segmento di rete dedicato, come una VLAN separata o una DMZ. Restringere rigorosamente il traffico in ingresso e in uscita da tale segmento, consentendo solo le comunicazioni strettamente necessarie, per limitare la superficie d'attacco e contenere eventuali compromissioni.

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 Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-2958 - CVSS 8.8 (ALTA)

È stata rilevata una vulnerabilità di sicurezza in D-Link DWR-M960 1.01.07. È interessata la funzione sub_457C5C del file /boafrm/formWsc. Tale manipolazione dell'argomento save_apply porta a un overflow del buffer basato su stack. L'attacco può essere eseguito da remoto. L'exploit è stato divulgato pubblicamente e può essere utilizzato.

Descrizione Originale (EN): A security vulnerability has been detected in D-Link DWR-M960 1.01.07. Affected is the function sub_457C5C of the file /boafrm/formWsc. Such manipulation of the argument save_apply leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.

Cosa può succedere?
Sfruttando questa vulnerabilità, un attaccante remoto può ottenere il controllo completo dei dispositivi D-Link interessati. Questo consente di accedere alla rete aziendale, rubare dati sensibili e causare interruzioni significative ai servizi critici.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	23/02/2026
Modificata:	23/02/2026
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 di rete rigorosi (firewall) per limitare l'esposizione del D-Link DWR-M960. Restringere l'accesso all'interfaccia di gestione del dispositivo unicamente a indirizzi IP o sottoreti amministrative fidate e interne, bloccando tentativi di connessione da reti non autorizzate. Ciò mitiga il rischio di sfruttamento remoto della vulnerabilità.

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 Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-2927 - CVSS 8.8 (ALTA)

È stata scoperta una vulnerabilità in D-Link DWR-M960 1.01.07. Questa vulnerabilità riguarda la funzione sub_462590 del file /boafrm/formOpMode del componente Operation Mode Configuration Endpoint. La manipolazione dell'argomento submit-url porta a un overflow del buffer basato su stack. L'attacco può essere avviato da remoto. L'exploit è stato divulgato al pubblico e può essere utilizzato.

Descrizione Originale (EN): A vulnerability has been found in D-Link DWR-M960 1.01.07. This vulnerability affects the function sub_462590 of the file /boafrm/formOpMode of the component Operation Mode Configuration Endpoint. The manipulation of the argument submit-url leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.

Cosa può succedere?

Un attaccante remoto può ottenere il controllo completo del router D-Link, compromettendo l'intera rete aziendale. Ciò può portare al furto di dati sensibili, all'interruzione dei servizi critici e all'esecuzione di ulteriori attacchi all'interno dell'infrastruttura.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.04% (Percentile: 0.14)
Pubblicata:	22/02/2026
Modificata:	22/02/2026
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 D-Link DWR-M960 su un segmento di rete dedicato, come una DMZ o una rete di gestione interna segregata, per limitarne l'esposizione. Implementare controlli di accesso stringenti sull'interfaccia amministrativa del dispositivo, consentendo connessioni solo da host di gestione fidati o tramite una VPN sicura.

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 Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-2928 - CVSS 8.8 (ALTA)

È stata individuata una vulnerabilità in D-Link DWR-M960 1.01.07. Questo problema riguarda la funzione sub_452CCC del file /boafrm/formWlEncrypt del componente WLAN Encryption Configuration Endpoint. La manipolazione dell'argomento submit-url provoca un buffer overflow 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 D-Link DWR-M960 1.01.07. This issue affects the function sub_452CCC of the file /boafrm/formWlEncrypt of the component WLAN Encryption Configuration Endpoint. The manipulation of the argument submit-url results in stack-based buffer overflow. The attack may be launched 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 router, compromettendo la sicurezza della rete aziendale. Ciò potrebbe causare il furto di dati sensibili, l'interruzione dei servizi essenziali e l'utilizzo del dispositivo per lanciare ulteriori attacchi.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.03% (Percentile: 0.07)
Pubblicata:	22/02/2026
Modificata:	22/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare il rischio, implementare controlli di accesso rigorosi sull'interfaccia di gestione del D-Link DWR-M960, consentendo l'accesso solo da indirizzi IP specifici e fidati all'interno di una rete di amministrazione segregata. Questa misura riduce significativamente la superficie di attacco remota e limita la possibilità di sfruttamento della vulnerabilità.

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 Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-2926 - CVSS 8.8 (ALTA)

È stata scoperta una vulnerabilità in D-Link DWR-M960 1.01.07. Questa interessa la funzione sub_4237AC del file /boafrm/formLteSetup del componente LTE Configuration Endpoint. L'esecuzione di una manipolazione dell'argomento submit-url può portare a un overflow del buffer basato su stack. L'attacco può essere eseguito da remoto. L'exploit è stato pubblicato e può essere utilizzato.

Descrizione Originale (EN): A flaw has been found in D-Link DWR-M960 1.01.07. This affects the function sub_4237AC of the file /boafrm/formLteSetup of the component LTE Configuration Endpoint. Executing a manipulation of the argument submit-url can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.

Cosa può succedere?

Sfruttando questa vulnerabilità, attaccanti remoti possono ottenere il controllo completo del router D-Link. Questo potrebbe causare l'intercettazione di dati sensibili, la compromissione della rete interna aziendale e l'interruzione dei servizi di connettività.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.04% (Percentile: 0.14)
Pubblicata:	22/02/2026
Modificata:	22/02/2026
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 router D-Link DWR-M960 posizionandola su una VLAN di gestione dedicata o dietro un firewall. Implementare regole firewall stringenti per limitare l'accesso a tale interfaccia solo da indirizzi IP interni fidati o host amministrativi specifici, impedendo così lo sfruttamento remoto da reti non attendibili.

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 Overflow, Stack Buffer Overflow

Approfondisci su VulnX

4 Vulnerabilità Critiche

5 Top 3 Minacce della Settimana

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

Minaccia #1: CVE-2020-7796 KEV

CVSS: 9.8/10 **EPSS:** 93.4% **Target:** Unknown **Rischio:** 9.7/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché è una vulnerabilità con un punteggio CVSS elevatissimo (9.8), un'altissima probabilità di sfruttamento (EPSS 93.4%) ed è attivamente sfruttata (CISA KEV).

Minaccia #2: CVE-2025-49113 KEV

CVSS: 9.9/10 **EPSS:** 90.0% **Target:** Unknown **Rischio:** 9.6/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché è attivamente sfruttata (CISA KEV), con un punteggio CVSS quasi massimo (9.9/10) e un'elevatissima probabilità di exploit (EPSS 90%), indicando un rischio immediato e grave.

Minaccia #3: CVE-2008-0015 KEV

CVSS: 8.8/10 **EPSS:** 80.6% **Target:** Unknown **Rischio:** 8.7/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica per via del suo alto punteggio CVSS (8.8) e dell'altissima probabilità di sfruttamento (EPSS 80.6%). È inoltre attivamente sfruttata e inclusa nel catalogo CISA KEV, indicando un rischio immediato e concreto.

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