VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Settimanale

02/02/2026 - 09/02/2026

Generato il: **09/02/2026 08:38**

Piattaforma Avanzata di Cyber Threat Intelligence

https://vulnx.it | Studio Consi

Chi Siamo

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

Vieni a scoprirci

Servizi Offerti

OSINT

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

Formazione

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

Vulnerability Assessment

Valutazione sistematica delle vulnerabilità presenti nei sistemi informativi.

Malware & Phishing Simulations

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

Penetration Testing

Test di penetrazione avanzati per simulare attacchi reali.

Consulenza UNI EN ISO

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

Quality of Service SOC

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

Consulenza Cybersecurity e Data Protection

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

Indice

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

2 Note Metodologiche **7**

3 Analisi delle Debolezze (CWE) **8**
3.1 Distribuzione CWE 8
3.2 Analisi Approfondita delle Debolezze (CWE) 8
3.3 CVE del Periodo Analizzato 14

4 Top 3 Minacce della Settimana **64**
4.1 EPSS Elevato (>95%) 65
4.2 Raccomandazioni 65
4.3 Risorse Aggiuntive 65

1 Sommario Esecutivo

INDICATORE DI RISCHIO SETTIMANALE

ALTO

Riepilogo Settimanale Livello di Minaccia:
Nella settimana corrente sono state registrate 1232 nuove CVE, di cui 120 classificate come critiche e 410 come ad alta gravità. Il catalogo KEV (Known Exploited Vulnerabilities) si è arricchito di 6 nuove voci, e una singola CVE presenta un punteggio EPSS superiore al 50%, indicando un'alta probabilità di exploit. **Azione Consigliata:** Si raccomanda di prioritizzare immediatamente la mitigazione delle 6 CVE presenti nel catalogo KEV e della CVE con EPSS >50%, data l'elevata probabilità di sfruttamento. È fondamentale mantenere un monitoraggio costante sulle vulnerabilità critiche e ad alta gravità per prevenire potenziali attacchi.

Metrica	Valore
Totale CVE	**1232**
Critiche	**120**
Alte	**410**
EPSS >50%	**1**
KEV	**6**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	1,226	–
CVE Modificate	2,135	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	120	11.0%
Alte (7.0-8.9)	410	37.8%
Medie (4.0-6.9)	473	43.6%
Basse (0.1-3.9)	83	7.6%
Indicatori di Rischio		
KEV (Exploit Attivi)	6	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.

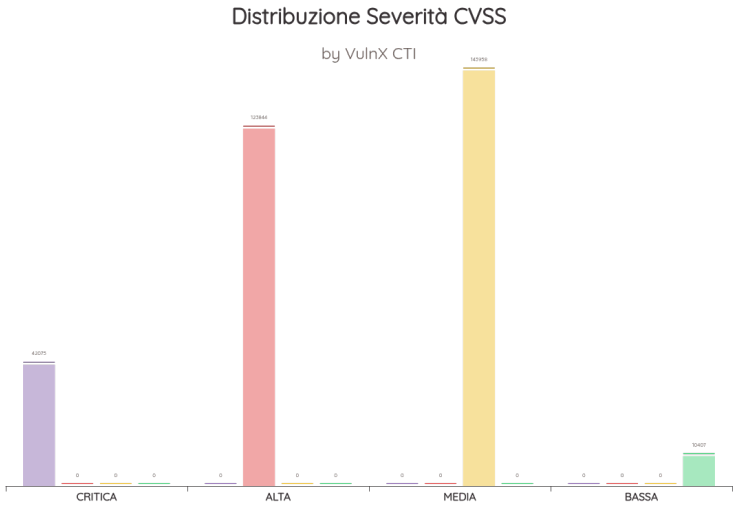
1.2 Panoramica Database (Storico Completo)

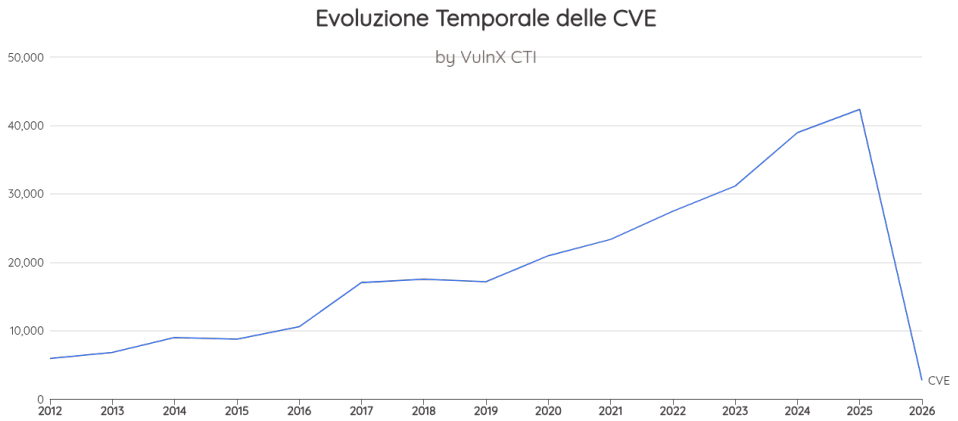
Statistiche complete del database storico su tutte le CVE mai pubblicate:

- **CVE Totali nel Database:** 331,699
- **KEV Totali (Vulnerabilità con Exploit Noti):** 1,509
- **CWE Totali Catalogate:** 969
- **CPE Totali Monitorati:** 2,186,309

Severità	Conteggio	Percentuale
CRITICA	42,075	13.1%
ALTA	123,844	38.7%
MEDIA	143,958	44.9%
BASSA	10,407	3.2%

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:

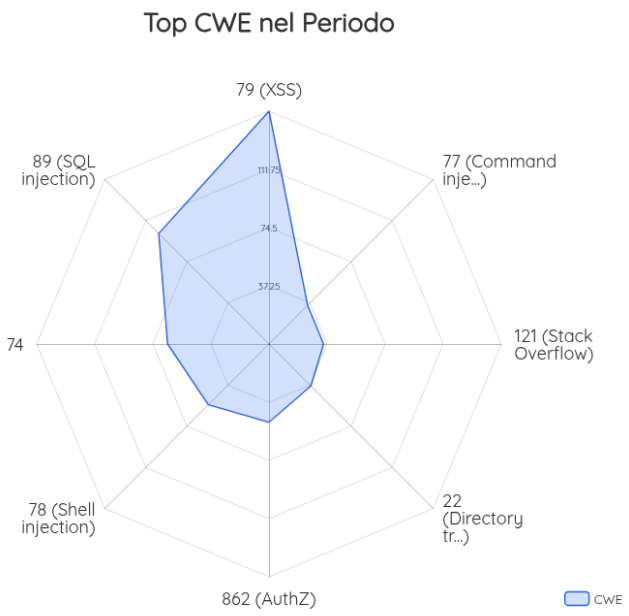


Figura 1: *Distribuzione Top CWE - Grafico Radar*

3.2 Analisi Approfondita delle Debolezze (CWE)

Le debolezze più comuni con raccomandazioni di difesa.

78

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

▶ **Occorrenze:** 55

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e pratiche per mitigare la CWE-78:
- N/A**Pratiche di Sviluppo:**Implementare una validazione rigorosa di tutti gli input utente (preferibilmente tramite *whitelisting*) prima del loro utilizzo in qualsiasi contesto che possa portare all'esecuzione di comandi di sistema.
- N/A**Pratiche di Sviluppo:**Evitare l'esecuzione diretta di comandi di sistema (es. 'system()', 'exec()'); preferire l'uso di API di sistema o librerie specifiche del linguaggio che offrono funzionalità equivalenti in modo più sicuro.
- N/A**Strumenti di Sicurezza/Configurazioni:**Configurare un Web Application Firewall (WAF) con regole specifiche per rilevare e bloccare i pattern noti di OS Command Injection nelle richieste HTTP.

121

Stack-based Buffer Overflow

- **Occorrenze:** 35

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-121 (Stack-based Buffer Overflow):
- N/A**Abilitare le protezioni dello stack (es. Stack Canaries)**: Configurare il compilatore per abilitare le protezioni dello stack (ad esempio, con flag come '-fstack-protector' per GCC/Clang o '/GS' per MSVC) che rilevano i tentativi di sovrascrittura dell'indirizzo di ritorno.
- N/A**Adottare pratiche di programmazione sicura**: Utilizzare funzioni di gestione della memoria sicure che prevengono gli overflow (es. 'strncpy_s', 'snprintf' invece di 'strcpy', 'sprintf') e implementare sempre il controllo dei limiti (bounds checking) su tutti gli input e le operazioni su buffer.
- N/A**Verificare e mantenere attive le protezioni OS**: Assicurarsi che le protezioni a livello di sistema operativo come DEP/NX (Data Execution Prevention/No-Execute) e ASLR (Address Space Layout Randomization) siano attive per mitigare l'esecuzione di codice arbitrario in caso di overflow.

77

Improper Neutralization of Special Elements used in a Command (’Command Injection’)

▶ **Occorrenze:** 35

Raccomandazioni di Difesa

- Ecco 2-3 raccomandazioni di difesa specifiche e attuabili per CWE-77 (Command Injection):
- N/A**Validazione Rigorosa degli Input:**Implementare una validazione stringente di tutti gli input utente, utilizzando liste bianche (whitelisting) per caratteri, formati e valori consentiti prima di qualsiasi elaborazione o esecuzione di comando.
- N/A**Utilizzo di API Sicure:**Evitare l’esecuzione diretta di comandi shell o l’interpolazione di stringhe in chiamate di sistema. Preferire l’utilizzo di API e librerie di sistema che eseguono funzioni specifiche senza invocare una shell (es. ‘subprocess.run‘ con ‘shell=False‘ in Python, ‘ProcessBuilder‘ in Java).
- N/A**Configurazione WAF:**Configurare il Web Application Firewall (WAF) con regole specifiche e aggiornate per rilevare e bloccare pattern noti di Command Injection e tentativi di esecuzione di comandi non autorizzati.

119

Improper Restriction of Operations within the Bounds of a Memory Buffer

▶ **Occorrenze:** 31

Raccomandazioni di Difesa

- Ecco 2-3 raccomandazioni specifiche e attuabili per CWE-119:
- N/A**Adottare pratiche di programmazione sicura**: Utilizzare funzioni di gestione della memoria e delle stringhe che includono controlli sui limiti (es. ‘strncpy‘, ‘snprintf‘ in C/C++) ed evitare quelle insicure (es. ‘strcpy‘, ‘sprintf‘). Preferire linguaggi con gestione automatica della memoria e dei limiti.
- N/A**Abilitare protezioni a livello di compilatore e sistema operativo**: Configurare e abilitare mitigazioni come ASLR (Address Space Layout Randomization), DEP/NX (Data Execution Prevention) e Stack Canaries/SSP (Stack Smashing Protection) per rendere più difficile lo sfruttamento dei buffer overflow.
- N/A**Implementare una rigorosa validazione degli input e analisi statica del codice (SAST)**: Validare e sanificare tutti gli input esterni per prevenire l’immissione di dati che possano causare overflow. Integrare strumenti SAST nel ciclo di sviluppo per identificare proattivamente vulnerabilità di buffer overflow nel codice.

428

Unquoted Search Path or Element

- **Occorrenze:** 27

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per mitigare la debolezza CWE-428:
- N/A**Pratiche di Sviluppo:**Nel ciclo di sviluppo, imporre la quotatura obbligatoria di tutti i percorsi che contengono spazi (es. “”C:\{}Program Files\{}App\{}app.exe”“) all’interno del codice sorgente, degli script e dei file di configurazione.
- N/A**Controlli di Sicurezza/Configurazione:**Implementare soluzioni di whitelisting delle applicazioni (es. AppLocker, Windows Defender Application Control) per consentire l’esecuzione solo di eseguibili autorizzati e firmati digitalmente, mitigando il rischio di esecuzione arbitraria da percorsi non quotati.
- N/A**Controlli di Rete/Configurazione:**Eseguire audit regolari dei servizi di sistema, delle attività pianificate e dei collegamenti rapidi su tutti i sistemi operativi (specialmente Windows) per identificare e correggere eventuali percorsi non quotati che puntano a file eseguibili.

209

Generation of Error Message Containing Sensitive Information

- **Occorrenze:** 5

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per mitigare la CWE-209:
- N/A**Sviluppare pagine di errore personalizzate e generiche:**Implementare messaggi di errore standardizzati che non rivelino dettagli tecnici sensibili (es. stack trace, percorsi di file, versioni software, query SQL) agli utenti finali.
- N/A**Configurare l'ambiente di produzione:**Disabilitare la visualizzazione di errori dettagliati (es. tramite 'display_errors=Off' in PHP, 'customErrors' in ASP.NET, o configurazioni simili del framework/server) e reindirizzare a pagine di errore generiche.
- N/A**Garantire logging interno degli errori:**Assicurarsi che i log di errore dettagliati siano scritti solo in file di log interni accessibili esclusivamente agli amministratori e non vengano mai esposti nelle risposte HTTP o nei messaggi utente.

3.3 CVE del Periodo Analizzato

Trovate **1226** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **25** CVE:

CVE-2026-1868 - CVSS 9.9 (CRITICA)

GitLab ha corretto una vulnerabilità nel componente Duo Workflow Service di GitLab AI Gateway che interessava tutte le versioni di AI Gateway dalla 18.1.6, 18.2.6, 18.3.1 fino alla 18.6.1, 18.7.0 e 18.8.0, in cui AI Gateway era vulnerabile a un'espansione insicura dei template dei dati forniti dall'utente tramite definizioni craftate di Duo Agent Platform Flow. Questa vulnerabilità poteva essere sfruttata per causare Denial of Service o ottenere l'esecuzione di codice sul Gateway. È stata risolta nelle versioni 18.6.2, 18.7.1 e 18.8.1 di GitLab AI Gateway.

Descrizione Originale (EN): GitLab has remediated a vulnerability in the Duo Workflow Service component of GitLab AI Gateway affecting all versions of the AI Gateway from 18.1.6, 18.2.6, 18.3.1 to 18.6.1, 18.7.0, and 18.8.0 in which AI Gateway was vulnerable to insecure template expansion of user supplied data via crafted Duo Agent Platform Flow definitions. This vulnerability could be used to cause Denial of Service or gain code execution on the Gateway. This has been fixed in versions 18.6.2, 18.7.1, and 18.8.1 of the GitLab AI Gateway.

Cosa può succedere?
Un'eventuale sfruttamento potrebbe causare l'interruzione dei servizi del Gateway AI di GitLab, rendendolo inutilizzabile. Nel caso più grave, un aggressore potrebbe eseguire codice malevolo sul sistema, ottenendone il controllo completo e compromettendo potenzialmente dati sensibili o altri sistemi aziendali.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	09/02/2026
Modificata:	09/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolate il componente GitLab AI Gateway in un segmento di rete dedicato, come una DMZ o una VLAN separata. Implementate regole firewall stringenti per permettere solo il traffico strettamente necessario da e verso l'AI Gateway, bloccando ogni connessione in uscita non essenziale che potrebbe essere sfruttata per esfiltrazione di dati o comando e controllo.

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

1336: **Improper Neutralization of Special Elements Used in a Template Engine**

Termini Alternativi: Server-Side Template Injection / SSTI, Client-Side Template Injection / CSTI

Approfondisci su VulnX

CVE-2026-1615 - CVSS 9.8 (CRITICA)

Tutte le versioni del pacchetto jsonpath sono vulnerabili a Arbitrary Code Injection tramite una valutazione non sicura delle espressioni JSON Path fornite dall'utente. La libreria si affida al modulo static-eval per elaborare l'input JSON Path, che non è progettato per gestire in modo sicuro dati non affidabili. Un attaccante può sfruttare questa vulnerabilità fornendo un'espressione JSON Path malevola che, quando valutata, esegue codice JavaScript arbitrario, portando a Remote Code Execution in ambienti Node.js o a Cross-site Scripting (XSS) in contesti browser. Ciò riguarda tutti i metodi che valutano JSON Path rispetto agli oggetti, inclusi .query, .nodes, .paths, .value, .parent e .apply.

Descrizione Originale (EN): All versions of the package jsonpath are vulnerable to Arbitrary Code Injection via unsafe evaluation of user-supplied JSON Path expressions. The library relies on the static-eval module to process JSON Path input, which is not designed to handle untrusted data safely. An attacker can exploit this vulnerability by supplying a malicious JSON Path expression that, when evaluated, executes arbitrary JavaScript code, leading to Remote Code Execution in Node.js environments or Cross-site Scripting (XSS) in browser contexts. This affects all methods that evaluate JSON Paths against objects, including .query, .nodes, .paths, .value, .parent, and .apply.

Cosa può succedere?
Un attaccante può eseguire codice arbitrario sui sistemi interessati, ottenendo il controllo completo. Ciò consente il furto di dati sensibili, l'interruzione dei servizi aziendali critici o la manipolazione e distruzione di informazioni.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	09/02/2026
Modificata:	09/02/2026
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 servizio che utilizza il pacchetto 'jsonpath' in un ambiente containerizzato o virtuale strettamente isolato. Assegnare a tale ambiente privilegi minimi di rete e di sistema (principio del minimo privilegio) per limitare drasticamente l'impatto di un'eventuale esecuzione di codice arbitrario e prevenire movimenti laterali nell'infrastruttura.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Approfondisci su VulnX

CVE-2026-2140 - CVSS 8.8 (ALTA)

È stata identificata una vulnerabilità in Tenda TX9 fino alla versione 22.03.02.10_multi. A rischio è la funzione sub_4223E0 del file /goform/setMacFilterCfg. Tale manipolazione dell'argomento deviceList porta a un buffer overflow. L'attacco può essere eseguito da remoto. L'exploit è disponibile pubblicamente e potrebbe essere utilizzato.

Descrizione Originale (EN): A vulnerability was identified in Tenda TX9 up to 22.03.02.10_multi. Affected by this issue is the function sub_4223E0 of the file /goform/setMacFilterCfg. Such manipulation of the argument deviceList leads to buffer overflow. The attack may be launched remotely. The exploit is publicly available and might be used.

Cosa può succedere?

L'exploit remoto di questa vulnerabilità permette a un attaccante di compromettere il router Tenda TX9, ottenendo il controllo della rete aziendale. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi critici e all'esecuzione di ulteriori attacchi.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.09% (Percentile: 0.25)
Pubblicata:	08/02/2026
Modificata:	08/02/2026
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 Tenda TX9 vulnerabili in un segmento di rete dedicato, separato dall'infrastruttura critica. Implementare rigorose regole del firewall per limitare l'accesso a questi dispositivi solo da host di gestione fidati e servizi interni strettamente necessari, riducendo drasticamente l'esposizione a potenziali attacchi remoti.

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

---

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

Probabilità di Sfruttamento: high

Termini Alternativi: Classic Buffer Overflow, Unbounded Transfer

Approfondisci su VulnX

CVE-2026-2139 - CVSS 8.8 (ALTA)

È stata individuata una vulnerabilità in Tenda TX9 fino alla versione 22.03.02.10_multi. La funzione interessata da questa vulnerabilità è sub_432580 del file /goform/fast_setting_wifi_set. Questa manipolazione dell'argomento ssid provoca un buffer overflow. L'attacco può essere avviato da remoto. L'exploit è stato divulgato pubblicamente e può essere utilizzato.

Descrizione Originale (EN): A vulnerability was determined in Tenda TX9 up to 22.03.02.10_multi. Affected by this vulnerability is the function sub_432580 of the file /goform/fast_setting_wifi_set. This manipulation of the argument ssid causes buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.

Cosa può succedere?
Un aggressore potrebbe ottenere il controllo completo dei router interessati. Ciò potrebbe causare interruzioni di rete, furto di dati sensibili o l'accesso non autorizzato alla rete interna aziendale.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.09% (Percentile: 0.25)
Pubblicata:	08/02/2026
Modificata:	08/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
In assenza di una patch, isolare il router Tenda TX9 in una VLAN dedicata o DMZ, separata dalle reti interne critiche. Implementare regole firewall restrittive per limitare il traffico in entrata e in uscita dal dispositivo, consentendo solo le comunicazioni strettamente necessarie per il suo funzionamento e prevenendo la propagazione di un 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

---

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

Probabilità di Sfruttamento: high

Termini Alternativi: Classic Buffer Overflow, Unbounded Transfer

Approfondisci su VulnX

CVE-2026-2138 - CVSS 8.8 (ALTA)

È stata riscontrata una vulnerabilità in Tenda TX9 fino alla versione 22.03.02.10_multi. È interessata la funzione sub_42D03C del file /goform/SetStaticRouteCfg. La manipolazione della lista degli argomenti provoca un buffer overflow. 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 TX9 up to 22.03.02.10_multi. Affected is the function sub_42D03C of the file /goform/SetStaticRouteCfg. The manipulation of the argument list results in buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.

Cosa può succedere?

Un aggressore potrebbe ottenere il pieno controllo del router e, di conseguenza, accedere alla rete interna dell'azienda. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi critici e alla compromissione di altri sistemi aziendali.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.09% (Percentile: 0.25)
Pubblicata:	08/02/2026
Modificata:	08/02/2026
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 patch e la natura remota dell'exploit pubblico, implementate una rigorosa segmentazione della rete per il dispositivo Tenda TX9. Collocate il router in una VLAN di gestione dedicata, limitando l'accesso alla sua interfaccia amministrativa esclusivamente a indirizzi IP specifici e autorizzati da workstation di gestione sicure. Questo ridurrà significativamente la superficie di attacco e la probabilità di sfruttamento remoto.

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

---

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

Probabilità di Sfruttamento: high

Termini Alternativi: Classic Buffer Overflow, Unbounded Transfer

Approfondisci su VulnX

CVE-2026-2137 - CVSS 8.8 (ALTA)

È stata individuata una vulnerabilità in Tenda TX3 fino alla versione 16.03.13.11_multi. Questa riguarda una funzione sconosciuta del file /goform/SetIpMacBind. La manipolazione dell'elenco degli argomenti porta a un buffer overflow. L'attacco può essere avviato da remoto. L'exploit è stato divulgato pubblicamente e potrebbe essere utilizzato.

Descrizione Originale (EN): A vulnerability has been found in Tenda TX3 up to 16.03.13.11_multi. This impacts an unknown function of the file /goform/SetIpMacBind. The manipulation of the argument list leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.

Cosa può succedere?

Un aggressore potrebbe ottenere il pieno controllo del router Tenda interessato, compromettendo l'intera rete aziendale. Ciò potrebbe causare furto di dati sensibili, interruzione dei servizi internet essenziali e l'utilizzo del dispositivo per lanciare ulteriori attacchi.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.09% (Percentile: 0.25)
Pubblicata:	08/02/2026
Modificata:	08/02/2026
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 natura remota della vulnerabilità, isolate immediatamente il dispositivo Tenda TX3 in un segmento di rete (VLAN) dedicato. Configurate regole firewall restrittive per consentire l'accesso alla sua interfaccia di gestione e alle porte critiche solo da host e reti strettamente necessarie e fidate, minimizzando così la superficie di 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

---

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

Probabilità di Sfruttamento: high

Termini Alternativi: Classic Buffer Overflow, Unbounded Transfer

Approfondisci su VulnX

CVE-2026-25632 - CVSS 10.0 (CRITICA)

EPyT-Flow è un pacchetto Python progettato per la generazione semplice di dati di scenario idraulico e qualità dell'acqua delle reti di distribuzione idrica. Prima della versione 0.16.1, l'API REST di EPyT-Flow analizzava i corpi richiesta JSON controllati dall'attaccante utilizzando un deserializer personalizzato (my_load_from_json) che supportava un campo type. Quando il campo era presente, il deserializer importava dinamicamente un modulo/classe specificato dall'attaccante e lo istanziava con argomenti forniti dall'attaccante. Ciò consentiva di invocare classi pericolose come subprocess.Popen, che potevano portare all'esecuzione di comandi OS durante l'analisi del JSON. Questo influiva anche sul caricamento di file JSON. Questa vulnerabilità è stata corretta in versione 0.16.1.

Descrizione Originale (EN): EPyT-Flow is a Python package designed for the easy generation of hydraulic and water quality scenario data of water distribution networks. Prior to 0.16.1, EPyT-Flow's REST API parses attacker-controlled JSON request bodies using a custom deserializer (my_load_from_json) that supports a type field. When type is present, the deserializer dynamically imports an attacker-specified module/class and instantiates it with attacker-supplied arguments. This allows invoking dangerous classes such as subprocess.Popen, which can lead to OS command execution during JSON parsing. This also affects the loading of JSON files. This vulnerability is fixed in 0.16.1.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo dei sistemi che utilizzano EPyT-Flow, permettendo l'esfiltrazione di dati sensibili o la manipolazione delle simulazioni idrauliche e della qualità dell'acqua. Ciò potrebbe causare interruzioni critiche dei servizi, compromissione dell'integrità dei dati e gravi danni all'infrastruttura aziendale.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.11% (Percentile: 0.29) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Posizionare un Web Application Firewall (WAF) davanti all'API REST di EPyT-Flow per ispezionare e filtrare il traffico JSON in ingresso. Configurare il WAF con regole specifiche per rilevare e bloccare pattern di attacchi di deserializzazione e l'uso anomalo o non autorizzato del campo 'type' nei corpi richiesta JSON.

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

502: **Deserialization of Untrusted Data**

Probabilità di Sfruttamento: medium

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

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25641 - CVSS 10.0 (CRITICA)

SandboxJS è una libreria di sandboxing JavaScript. Prima della versione 0.8.29, esiste una vulnerabilità di escape del sandbox dovuta a una discrepanza tra la chiave su cui viene eseguita la validazione e la chiave utilizzata per accedere alle proprietà. Anche se la chiave utilizzata negli accessi alle proprietà è annotata come stringa, questa non viene mai applicata in modo effettivo. Di conseguenza, gli attaccanti possono passare oggetti dannosi che si coerciscono in valori stringa differenti quando vengono utilizzati, ad esempio, uno per il momento in cui la chiave viene sanificata tramite hasOwnProperty(key) e un altro per quando la chiave viene usata per l'accesso effettivo alla proprietà. Questa vulnerabilità è stata corretta in versione 0.8.29.

Descrizione Originale (EN): SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, there is a sandbox escape vulnerability due to a mismatch between the key on which the validation is performed and the key used for accessing properties. Even though the key used in property accesses is annotated as string, this is never enforced. So, attackers can pass malicious objects that coerce to different string values when used, e.g., one for the time the key is sanitized using hasOwnProperty(key) and a different one for when the key is used for the actual property access. This vulnerability is fixed in 0.8.29.

Cosa può succedere?
Gli attaccanti potrebbero ottenere il controllo completo dei sistemi che utilizzano la libreria SandboxJS, evadendo l'ambiente protetto. Ciò consentirebbe il furto di dati sensibili, la compromissione dei servizi aziendali e gravi interruzioni operative.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.04% (Percentile: 0.11) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare una segmentazione di rete rigorosa per isolare i sistemi che utilizzano la libreria SandboxJS da reti più sensibili. Questo limiterà significativamente la capacità di un attaccante di muoversi lateralmente e accedere a risorse critiche in caso di successo di un'evasione della sandbox.

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

367: **Time-of-check Time-of-use (TOCTOU) Race Condition**

Probabilità di Sfruttamento: medium

Termini Alternativi: TOCTTOU, TOCCTOU

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25587 - CVSS 10.0 (CRITICA)

SandboxJS è una libreria di sandboxing JavaScript. Prima della versione 0.8.29, poiché Map si trova in SAFE_PROTOYPES, il suo prototype può essere ottenuto tramite Map.prototype. Sovrascrivendo Map.prototype.has, è possibile sfuggire al sandbox. Questa vulnerabilità è stata corretta in versione 0.8.29.

Descrizione Originale (EN): SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, as Map is in SAFE_PROTOYPES, it's prototype can be obtained via Map.prototype. By overwriting Map.prototype.has the sandbox can be escaped. This vulnerability is fixed in 0.8.29.

Cosa può succedere?

Sfruttando questa vulnerabilità, un attaccante può sfuggire al sandbox JavaScript e ottenere il controllo del sistema sottostante. Ciò potrebbe causare il furto di dati sensibili, la compromissione completa dell'infrastruttura o l'interruzione dei servizi aziendali critici.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.05% (Percentile: 0.15) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Eseguire l'applicazione che utilizza SandboxJS con i privilegi minimi indispensabili sul sistema operativo host. Questo limita drasticamente le azioni che un attaccante può compiere anche dopo aver eluso la sandbox, riducendo significativamente il potenziale impatto di una compromissione.

CVSS Metrics

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

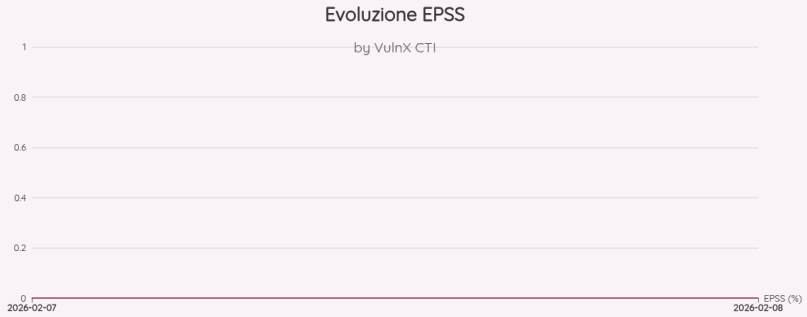
CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-25586 - CVSS 10.0 (CRITICA)

SandboxJS è una libreria di sandboxing JavaScript. Prima della versione 0.8.29, era possibile sfuggire al sandbox shadowando hasOwnProperty su un oggetto sandbox, il che disabilitava l'applicazione della whitelist del prototype nel percorso di accesso alle proprietà. Ciò consentiva l'accesso diretto a __proto__ e ad altre proprietà del prototype bloccate, permettendo l'inquinamento di Object.prototype da parte dell'host e un impatto persistente tra sandbox. Questa vulnerabilità è stata corretta in versione 0.8.29.

Descrizione Originale (EN): SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, a sandbox escape is possible by shadowing hasOwnProperty on a sandbox object, which disables prototype whitelist enforcement in the property-access path. This permits direct access to __proto__ and other blocked prototype properties, enabling host Object.prototype pollution and persistent cross-sandbox impact. This vulnerability is fixed in 0.8.29.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo del sistema o dell'applicazione, superando le restrizioni di sicurezza. Ciò potrebbe portare al furto di dati sensibili, alla manipolazione di informazioni cruciali o all'interruzione persistente dei servizi aziendali.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.05% (Percentile: 0.15) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare le applicazioni che utilizzano la libreria SandboxJS vulnerabile all'interno di un segmento di rete dedicato con un filtraggio in uscita (egress filtering) rigoroso. Questa misura limita la potenziale movimentazione laterale e l'accesso ad altre risorse interne, contenendo l'impatto di un exploit riuscito anche in caso di fuga dalla sandbox.

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

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

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25520 - CVSS 10.0 (CRITICA)

SandboxJS è una libreria di sandboxing JavaScript. Prima della versione 0.8.29, i valori di ritorno delle funzioni non sono avvolti. Object.values/Object.entries possono essere utilizzati per ottenere un Array contenente il costruttore Function dell'host; utilizzando Array.prototype.at si può ottenere il costruttore Function dell'host, che può essere usato per eseguire codice arbitrario al di fuori del sandbox. Questa vulnerabilità è stata corretta in versione 0.8.29.

Descrizione Originale (EN): SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, The return values of functions aren't wrapped. Object.values/Object.entries can be used to get an Array containing the host's Function constructor, by using Array.prototype.at you can obtain the hosts Function constructor, which can be used to execute arbitrary code outside of the sandbox. This vulnerability is fixed in 0.8.29.

Cosa può succedere?

Un aggressore potrebbe eseguire codice arbitrario sul sistema, ottenendo il controllo completo e rubando dati sensibili come informazioni sui clienti o proprietà intellettuale. Questo potrebbe causare gravi interruzioni dei servizi, danni alla reputazione e la compromissione di altri sistemi aziendali.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.08% (Percentile: 0.23) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolate i sistemi che utilizzano la libreria SandboxJS in un segmento di rete dedicato e altamente ristretto. Applicate rigorose politiche di firewall che permettano solo le comunicazioni essenziali per limitare la capacità di un eventuale codice malevolo di propagarsi o esfiltrare dati dall'infrastruttura. Questo ridurrà significativamente il raggio d'azione di un attacco anche in caso di exploit riuscito.

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

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

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-1731 - CVSS 9.9 (CRITICA)

BeyondTrust Remote Support (RS) e alcune versioni più vecchie di Privileged Remote Access (PRA) presentano una vulnerabilità critica di esecuzione di codice remoto pre-autenticazione. Inviando richieste appositamente formulate, un attaccante remoto non autenticato potrebbe essere in grado di eseguire comandi del sistema operativo nel contesto dell'utente del sito.

Descrizione Originale (EN): BeyondTrust Remote Support (RS) and certain older versions of Privileged Remote Access (PRA) contain a critical pre-authentication remote code execution vulnerability. By sending specially crafted requests, an unauthenticated remote attacker may be able to execute operating system commands in the context of the site user.

Cosa può succedere?

Un attaccante remoto non autenticato può ottenere il pieno controllo dei sistemi BeyondTrust vulnerabili. Questo permette il furto di dati sensibili, gravi interruzioni dei servizi critici e la potenziale diffusione dell'attacco all'intera rete aziendale.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.44% (Percentile: 0.63) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare una rigorosa segmentazione di rete per le istanze di BeyondTrust Remote Support e Privileged Remote Access. Limitare l'accesso di rete a questi sistemi esclusivamente alle sottoreti amministrative interne fidate o a specifici indirizzi IP, riducendo al minimo la loro esposizione a reti non attendibili come Internet. Questa misura diminuisce drasticamente la superficie di attacco per aggressori remoti non autenticati.

CVSS Metrics

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

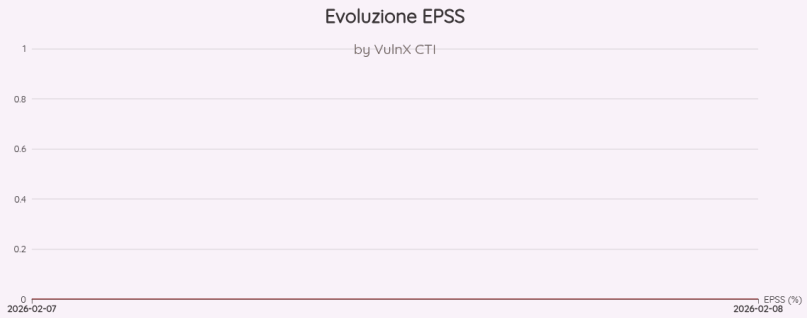
CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

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

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-25592 - CVSS 9.9 (CRITICA)

Semantic Kernel è un SDK utilizzato per costruire, orchestrare e distribuire agent AI e sistemi multi-agent. Prima della versione 1.70.0, è stata identificata una vulnerabilità di Arbitrary File Write nel SDK .NET di Microsoft's Semantic Kernel, specificamente all'interno di SessionsPythonPlugin. Il problema è stato risolto nella versione 1.70.0 di Microsoft.SemanticKernel.Core. Come misura di mitigazione, gli utenti possono creare un Function Invocation Filter che verifica gli argomenti passati a qualsiasi chiamata a DownloadFileAsync o UploadFileAsync e garantisce che il percorso del file locale fornito sia presente in una whitelist.

Descrizione Originale (EN): Semantic Kernel is an SDK used to build, orchestrate, and deploy AI agents and multi-agent systems. Prior to 1.70.0, an Arbitrary File Write vulnerability has been identified in Microsoft's Semantic Kernel .NET SDK, specifically within the SessionsPythonPlugin. The problem has been fixed in Microsoft.SemanticKernel.Core version 1.70.0. As a mitigation, users can create a Function Invocation Filter which checks the arguments being passed to any calls to DownloadFileAsync or UploadFileAsync and ensures the provided localFilePath is allow listed.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo dei sistemi che utilizzano l'SDK Semantic Kernel, permettendo il furto di dati sensibili o la manipolazione degli agenti AI. Questo potrebbe causare gravi interruzioni operative e compromettere l'integrità dei processi aziendali che si affidano a tali sistemi.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	0.10% (Percentile: 0.27) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Adottare il principio del minimo privilegio per l'applicazione che utilizza Semantic Kernel. Assicurarsi che il processo dell'applicazione abbia permessi di scrittura limitati esclusivamente alle directory strettamente necessarie per il suo funzionamento, prevenendo così la scrittura arbitraria di file in aree sensibili del sistema.

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

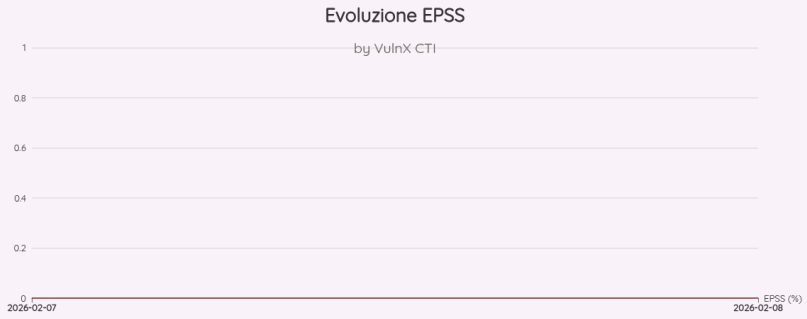
CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Termini Alternativi: Directory traversal, Path traversal

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2025-15027 - CVSS 9.8 (CRITICA)

Il plugin JAY Login & Register per WordPress è vulnerabile a Privilege Escalation in tutte le versioni fino, e inclusa, 2.6.03. Ciò è dovuto al fatto che il plugin consente a un utente di aggiornare metadati utente arbitrari tramite la funzione 'jay_login_register_ajax_create_final_user'. Questo rende possibile agli attaccanti non autenticati elevare i propri privilegi a quelli di amministratore.

Descrizione Originale (EN): The JAY Login & Register plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.6.03. This is due to the plugin allowing a user to update arbitrary user meta through the 'jay_login_register_ajax_create_final_user' function. This makes it possible for unauthenticated attackers to elevate their privileges to that of an administrator.

Cosa può succedere?

Gli attaccanti non autenticati possono ottenere il pieno controllo del sito WordPress, accedendo a dati sensibili di utenti e clienti. Questo può comportare furto di informazioni, interruzione dei servizi web e danni significativi alla reputazione aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.07% (Percentile: 0.22)
Pubblicata:	08/02/2026
Modificata:	08/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un Web Application Firewall (WAF) per monitorare e filtrare il traffico HTTP/S diretto all'istanza WordPress. Configurare il WAF per rilevare e bloccare tentativi di manipolazione dei metadati utente o chiamate sospette alla funzione 'jay_login_register_ajax_create_final_user', prevenendo così l'escalation di privilegi 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

269: **Improper Privilege Management**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2020-37159 - CVSS 9.8 (CRITICA)

Parallaxis Cuckoo Clock 5.0 presenta una vulnerabilità di buffer overflow che consente agli attaccanti di eseguire codice arbitrario sovrascrivendo i registri di memoria nella funzione di pianificazione dell'allarme. Gli attaccanti possono creare un payload dannoso superiore a 260 byte per sovrascrivere EIP e EBP, abilitando l'esecuzione di shellcode con potenziale esecuzione di codice remoto.

Descrizione Originale (EN): Parallaxis Cuckoo Clock 5.0 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting memory registers in the alarm scheduling feature. Attackers can craft a malicious payload exceeding 260 bytes to overwrite EIP and EBP, enabling shellcode execution with potential remote code execution.

Cosa può succedere?

Gli attaccanti potrebbero ottenere il controllo completo dei sistemi aziendali vulnerabili, consentendo il furto di dati sensibili o la distruzione di informazioni critiche. Ciò causerebbe gravi interruzioni operative, potenziali perdite finanziarie e danni reputazionali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.18% (Percentile: 0.39) Disponibili 2 valori storici
Pubblicata:	07/02/2026
Modificata:	07/02/2026
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 sistema che esegue Parallaxis Cuckoo Clock 5.0 in un segmento di rete dedicato (ad esempio, una VLAN o una zona demilitarizzata) con regole firewall rigorose. Questo limiterà le connessioni in entrata e in uscita al minimo indispensabile, contenendo l'impatto di un'eventuale esecuzione di codice arbitrario e prevenendo la propagazione laterale.

CVSS Metrics

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

CWE - Common Weakness Enumeration

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2020-37162 - CVSS 9.8 (CRITICA)

Wedding Slideshow Studio 1.36 presenta una vulnerabilità di overflow del buffer nell'inserimento della chiave di registrazione che consente agli attaccanti di eseguire codice arbitrario sovrascrivendo la memoria. Gli aggressori possono creare un payload dannoso di 1608 byte per attivare un overflow del buffer basato su stack ed eseguire comandi tramite il campo della chiave di registrazione.

Descrizione Originale (EN): Wedding Slideshow Studio 1.36 contains a buffer overflow vulnerability in the registration key input that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious payload of 1608 bytes to trigger a stack-based buffer overflow and execute commands through the registration key field.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo del sistema affetto, consentendo il furto di dati sensibili, l'interruzione dei servizi critici o l'installazione di software dannoso come ransomware. Ciò potrebbe causare gravi perdite finanziarie e danni significativi alla reputazione aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.05% (Percentile: 0.16) Disponibili 2 valori storici
Pubblicata:	07/02/2026
Modificata:	07/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementate una rigorosa whitelisting delle applicazioni (application whitelisting) su tutti gli endpoint per impedire l'esecuzione di software non autorizzato o non essenziale, incluso Wedding Slideshow Studio. Questo previene l'attivazione della vulnerabilità bloccando l'esecuzione dell'applicazione stessa o di codice arbitrario.

CVSS Metrics

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

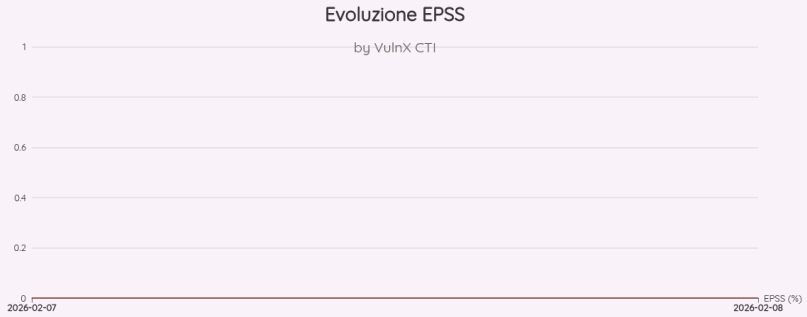
CWE - Common Weakness Enumeration

122: **Heap-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Heap Overflow, Heap Buffer Overflow

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2020-37161 - CVSS 9.8 (CRITICA)

Wedding Slideshow Studio 1.36 presenta una vulnerabilità di buffer overflow che consente agli attaccanti di eseguire codice arbitrario sovrascrivendo il campo nome registrazione con payload dannoso. Gli attaccanti possono creare un payload appositamente progettato per attivare l'esecuzione di codice remoto, dimostrando la capacità di eseguire comandi di sistema come l'apertura della calcolatrice.

Descrizione Originale (EN): Wedding Slideshow Studio 1.36 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting the registration name field with malicious payload. Attackers can craft a specially designed payload to trigger remote code execution, demonstrating the ability to run system commands like launching the calculator.

Cosa può succedere?

Sfruttando questa vulnerabilità, un attaccante può ottenere il controllo completo del sistema interessato. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi aziendali critici o all'installazione di software dannoso, compromettendo gravemente l'integrità e la disponibilità delle operazioni.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.18% (Percentile: 0.39) Disponibili 2 valori storici
Pubblicata:	07/02/2026
Modificata:	07/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Adottare un controllo degli accessi rigoroso e il principio del minimo privilegio per gli account utente che utilizzano l'applicazione Wedding Slideshow Studio. Implementare inoltre la whitelisting delle applicazioni (application whitelisting) sugli endpoint per impedire l'esecuzione di codice non autorizzato, anche in caso di sfruttamento della vulnerabilità di buffer overflow.

CVSS Metrics

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

CWE - Common Weakness Enumeration

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2020-37095 - CVSS 9.8 (CRITICA)

Cyberoam Authentication Client 2.1.2.7 contiene una vulnerabilità di buffer overflow che consente agli attaccanti remoti di eseguire codice arbitrario sovrascrivendo la memoria del Structured Exception Handler (SEH). Gli attaccanti possono creare un input dannoso nel campo 'Cyberoam Server Address' per attivare una shell TCP bind sulla porta 1337 con accesso a livello di sistema.

Descrizione Originale (EN): Cyberoam Authentication Client 2.1.2.7 contains a buffer overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) memory. Attackers can craft a malicious input in the 'Cyberoam Server Address' field to trigger a bind TCP shell on port 1337 with system-level access.

Cosa può succedere?

Un attaccante remoto potrebbe ottenere il controllo completo dei sistemi aziendali vulnerabili, consentendo l'accesso, la modifica o il furto di dati sensibili. Questo potrebbe causare interruzioni gravi ai servizi operativi e compromettere l'intera infrastruttura IT, con rischi elevati per la continuità del business e la reputazione.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.39% (Percentile: 0.60) Disponibili 2 valori storici
Pubblicata:	07/02/2026
Modificata:	07/02/2026
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 patch, isolate i sistemi che eseguono il Cyberoam Authentication Client in un segmento di rete dedicato e strettamente controllato. Implementate regole firewall restrittive per bloccare tutte le connessioni in entrata non essenziali verso tali sistemi, in particolare sulla porta 1337, e limitate le connessioni in uscita solo ai server Cyberoam e alle risorse autorizzate.

CVSS Metrics

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

CWE - Common Weakness Enumeration

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-25803 - CVSS 9.8 (CRITICA)

3DP-MANAGER è un generatore inbound per 3x-ui. Nella versione 2.0.1 e precedenti, l'applicazione crea automaticamente un account amministrativo con credenziali di default note (admin/admin) al primo avvio. Gli attaccanti con accesso alla rete all'interfaccia di login dell'applicazione possono ottenere il controllo amministrativo completo, gestendo tunnel VPN e impostazioni di sistema. Questo problema sarà risolto nella versione 2.0.2.

Descrizione Originale (EN): 3DP-MANAGER is an inbound generator for 3x-ui. In version 2.0.1 and prior, the application automatically creates an administrative account with known default credentials (admin/admin) upon the first initialization. Attackers with network access to the application's login interface can gain full administrative control, managing VPN tunnels and system settings. This issue will be patched in version 2.0.2.

Cosa può succedere?

Gli attaccanti possono ottenere il controllo amministrativo completo dei sistemi, consentendo il furto di dati sensibili, l'interruzione dei servizi critici (come le VPN) e la compromissione totale dell'infrastruttura aziendale. Questo può portare a gravi perdite finanziarie e danni alla reputazione.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
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, isolare l'istanza di 3DP-MANAGER in un segmento di rete o VLAN dedicato. Limitare l'accesso alla sua interfaccia di gestione esclusivamente a indirizzi IP specifici e autorizzati, consentendo l'accesso solo agli amministratori da una rete di gestione sicura o tramite jump host.

CVSS Metrics

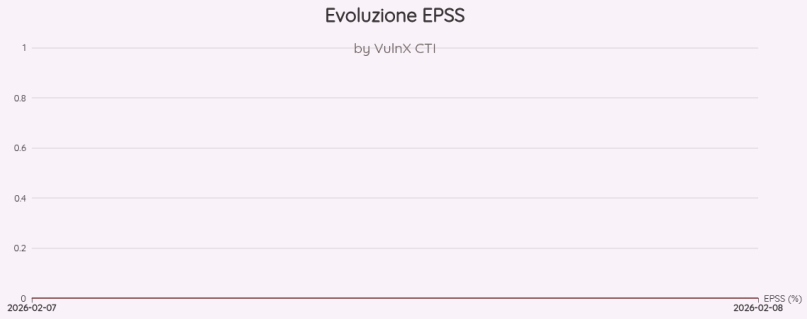
- **Vettore di Attacco:** network
- **Complessità di Attacco:** low
- **Privilegi Richiesti:** none
- **Interazione Utente:** none
- **Ambito:** unchanged
- **Impatto Confidenzialità:** high
- **Impatto Integrità:** high
- **Impatto Disponibilità:** high

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-25544 - CVSS 9.8 (CRITICA)

Payload è un sistema di gestione dei contenuti headless, open source e gratuito. Prima della versione 3.73.0, quando si interrogavano campi JSON o richText, l'input dell'utente veniva inserito direttamente in SQL senza escaping, consentendo attacchi di SQL injection cieca. Un attaccante non autenticato poteva estrarre dati sensibili (email, token di reset password) e ottenere il pieno controllo dell'account senza dover crackare la password. Questa vulnerabilità è stata corretta in 3.73.0.

Descrizione Originale (EN): Payload is a free and open source headless content management system. Prior to 3.73.0, when querying JSON or richText fields, user input was directly embedded into SQL without escaping, enabling blind SQL injection attacks. An unauthenticated attacker could extract sensitive data (emails, password reset tokens) and achieve full account takeover without password cracking. This vulnerability is fixed in 3.73.0.

Cosa può succedere?

Un attaccante non autenticato può rubare dati sensibili degli utenti, inclusi email e token di reset password, ottenendo il controllo completo dei loro account. Questo può portare a gravi violazioni della privacy, furto d'identità e compromissione dei sistemi aziendali, con conseguenti significative perdite finanziarie e danni reputazionali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.05% (Percentile: 0.16) Disponibili 2 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
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) di fronte all'istanza di Payload CMS. Configurare il WAF per ispezionare e bloccare attivamente le richieste che contengono pattern noti di SQL injection, mitigando così il rischio di sfruttamento della vulnerabilità da parte di attaccanti non autenticati.

CVSS Metrics

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

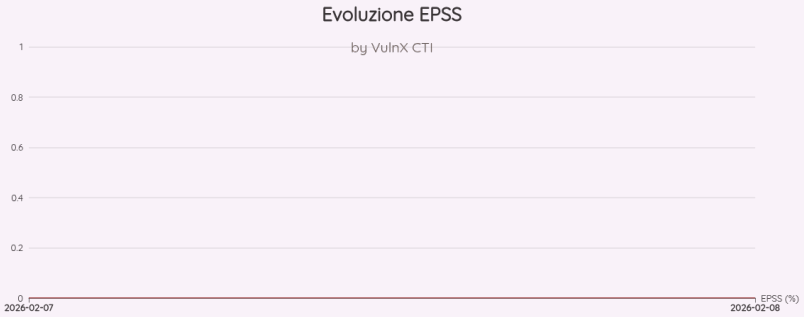
CWE - Common Weakness Enumeration

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-2026-2017 - CVSS 9.8 (CRITICA)

Una vulnerabilità è stata rilevata in IP-COM W30AP fino alla versione 1.0.0.11(1340). Affected by this issue is the function R7WebsSecurityHandler del file /goform/wx3auth del componente POST Request Handler. La manipolazione del dato dell'argomento provoca un buffer overflow basato su stack. L'attacco può essere eseguito da remoto. L'exploit è ora pubblico e può essere utilizzato. Il fornitore è stato contattato tempestivamente riguardo a questa divulgazione, ma non ha risposto in alcun modo.

Descrizione Originale (EN): A vulnerability was detected in IP-COM W30AP up to 1.0.0.11(1340). Affected by this issue is the function R7WebsSecurityHandler of the file /goform/wx3auth of the component POST Request Handler. The manipulation of the argument data results in stack-based buffer overflow. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?
L'exploit di questa vulnerabilità critica consente a un attaccante remoto di ottenere il controllo completo del dispositivo. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi di rete o all'utilizzo del dispositivo come punto di accesso per ulteriori attacchi all'infrastruttura aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.08% (Percentile: 0.24) Disponibili 3 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
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 IP-COM W30AP su una VLAN dedicata o un segmento di rete separato. Implementare regole firewall stringenti per limitare l'accesso in ingresso alla loro interfaccia di gestione esclusivamente da reti amministrative fidate, riducendo significativamente la superficie di attacco remoto.

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

---

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-21643 - CVSS 9.8 (CRITICA)

Una vulnerabilità di neutralizzazione impropria di elementi speciali utilizzati in un comando SQL ('sql injection') in Fortinet FortiClientEMS 7.4.4 potrebbe consentire a un attaccante non autenticato di eseguire codice o comandi non autorizzati tramite richieste HTTP appositamente manipolate.

Descrizione Originale (EN): An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiClientEMS 7.4.4 may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.

Cosa può succedere?

Un attaccante non autenticato potrebbe ottenere il controllo completo del sistema FortiClientEMS. Ciò permetterebbe il furto di dati sensibili, l'interruzione dei servizi critici e l'esecuzione di attacchi successivi all'interno della rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.13% (Percentile: 0.33) Disponibili 3 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare questa vulnerabilità critica, implementare immediatamente un Web Application Firewall (WAF) davanti al server FortiClientEMS. Configurare il WAF per ispezionare e bloccare attivamente le richieste HTTP malevole che tentano iniezioni SQL e altre tecniche di attacco web, limitando drasticamente l'esposizione del servizio.

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-2026-1499 - CVSS 9.8 (CRITICA)

Il plugin WP Duplicate per WordPress è vulnerabile a Missing Authorization che può portare a Arbitrary File Upload in tutte le versioni fino alla 1.1.8 inclusa. Ciò è dovuto a una mancanza di controllo delle capacità sull'azione AJAX 'process_add_site()' combinata con una vulnerabilità di path traversal nella funzionalità di caricamento dei file. Questo rende possibile a un attaccante autenticato (a livello di subscriber) impostare l'opzione interna 'prod_key_random_id', che può poi essere utilizzata da un attaccante non autenticato per bypassare i controlli di autenticazione e scrivere file arbitrari sul server tramite la funzione 'handle_upload_single_big_file()', portando infine all'esecuzione di codice remoto.

Descrizione Originale (EN): The WP Duplicate plugin for WordPress is vulnerable to Missing Authorization leading to Arbitrary File Upload in all versions up to and including 1.1.8. This is due to a missing capability check on the 'process_add_site()' AJAX action combined with path traversal in the file upload functionality. This makes it possible for authenticated (subscriber-level) attackers to set the internal 'prod_key_random_id' option, which can then be used by an unauthenticated attacker to bypass authentication checks and write arbitrary files to the server via the 'handle_upload_single_big_file()' function, ultimately leading to remote code execution.

Cosa può succedere?

Un attaccante autenticato, anche con privilegi minimi, potrebbe prendere il controllo completo del sito WordPress. Questo consentirebbe il furto di dati sensibili, la modifica dei contenuti o l'interruzione dei servizi, con gravi ripercussioni sulla reputazione e sulle operazioni aziendali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	1.23% (Percentile: 0.79) Disponibili 3 valori storici
Pubblicata:	06/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Configurare un Web Application Firewall (WAF) per monitorare e bloccare attivamente le richieste all'endpoint '/wp-admin/admin-ajax.php' che tentano di caricare file o sfruttare vulnerabilità di path traversal. Questo funge da controllo compensativo essenziale per mitigare la vulnerabilità di caricamento file arbitrario, anche da parte di un utente autenticato, fino a quando non sarà disponibile 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

862: **Missing Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-24300 - CVSS 9.8 (CRITICA)

Vulnerabilità di Elevation of Privilege di Azure Front Door

Descrizione Originale (EN): Azure Front Door Elevation of Privilege Vulnerability

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo sui servizi Azure Front Door, reindirizzando il traffico. Ciò potrebbe portare a interruzioni gravi dei servizi web, furto di dati sensibili o compromissione di sistemi aziendali critici.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.09% (Percentile: 0.25) Disponibili 3 valori storici
Pubblicata:	05/02/2026
Modificata:	06/02/2026
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 di Elevation of Privilege in Azure Front Door e l'assenza di una patch, è cruciale rafforzare i controlli compensativi. Rivedere e rafforzare rigorosamente i controlli di accesso basati sui ruoli (RBAC) applicati alla configurazione di Azure Front Door e alle risorse backend che protegge, aderendo al principio del minimo privilegio. Assicurarsi che solo le identità strettamente necessarie (utenti, gruppi, Managed Identities) abbiano i permessi essenziali per prevenire e limitare l'impatto di qualsiasi potenziale escalation di privilegi.

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

284: **Improper Access Control**

Termini Alternativi: Authorization

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2025-70073 - CVSS 9.8 (CRITICA)

Una vulnerabilità in ChestnutCMS v.1.5.8 e versioni precedenti consente a un attaccante remoto di eseguire codice arbitrario tramite la funzione di creazione dei template

Descrizione Originale (EN): An issue in ChestnutCMS v.1.5.8 and before allows a remote attacker to execute arbitrary code via the template creation function

Cosa può succedere?

Un attaccante remoto potrebbe ottenere il controllo completo del server, rubando dati sensibili come informazioni sui clienti o finanziarie. Ciò causerebbe interruzioni dei servizi critici e potrebbe portare alla diffusione dell'attacco all'intera rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.25% (Percentile: 0.48) Disponibili 3 valori storici
Pubblicata:	05/02/2026
Modificata:	06/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) davanti al server ChestnutCMS. Configurare il WAF per ispezionare e bloccare proattivamente tentativi di iniezione di codice o attività sospette nelle richieste HTTP dirette alla funzione di creazione dei template, mitigando attacchi di esecuzione di codice remoto.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

4 Top 3 Minacce della Settimana

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

Minaccia #1: CVE-2019-19006 KEV

CVSS: 9.8/10 **EPSS:** 31.6% **Target:** Unknown **Rischio:** 7.8/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché, con un CVSS di 9.8/10, è attivamente sfruttata (CISA KEV) e presenta una significativa probabilità di exploit (EPSS 31.6%).

Minaccia #2: CVE-2025-40551 KEV

CVSS: 9.8/10 **EPSS:** 22.9% **Target:** Unknown **Rischio:** 7.6/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché, con un punteggio CVSS di 9.8, è attivamente sfruttata (come indicato dallo stato KEV di CISA) e presenta una significativa probabilità di exploit.

Minaccia #3: CVE-2026-24423 KEV

CVSS: 9.8/10 **EPSS:** 9.2% **Target:** Unknown **Rischio:** 7.2/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché il suo punteggio CVSS di 9.8 indica una vulnerabilità estremamente grave ed è attivamente sfruttata (CISA KEV), richiedendo un'azione immediata.

4.1 EPSS Elevato (>95%)

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

4.2 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**

4.3 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