VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Settimanale

09/02/2026 - 16/02/2026

Generato il: **16/02/2026 07:12**

Piattaforma Avanzata di Cyber Threat Intelligence

https://vulnx.it | Studio Consi

Chi Siamo

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

Vieni a scoprirci

Servizi Offerti

OSINT

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

Formazione

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

Vulnerability Assessment

Valutazione sistematica delle vulnerabilità presenti nei sistemi informativi.

Malware & Phishing Simulations

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

Penetration Testing

Test di penetrazione avanzati per simulare attacchi reali.

Consulenza UNI EN ISO

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

Quality of Service SOC

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

Consulenza Cybersecurity e Data Protection

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

Indice

1 Sommario Esecutivo

INDICATORE DI RISCHIO SETTIMANALE

ALTO

Riepilogo Settimanale Livello di Minaccia:
Questa settimana sono state identificate 1245 nuove CVE, di cui 96 classificate come critiche e 400 come alte. Si evidenzia la presenza di 11 nuove vulnerabilità nel catalogo KEV e 3 con un punteggio EPSS superiore al 50%, indicando un'alta probabilità di exploit nel prossimo futuro. **Azione Consigliata:** Si raccomanda di prioritizzare immediatamente la mitigazione delle 96 CVE critiche e delle 11 KEV, monitorando attentamente le 3 vulnerabilità con alta probabilità di exploit per prevenire potenziali compromissioni.

Metrica	Valore
Totale CVE	**1245**
Critiche	**96**
Alte	**400**
EPSS >50%	**3**
KEV	**11**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	1,242	–
CVE Modificate	1,934	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	96	9.5%
Alte (7.0-8.9)	400	39.5%
Medie (4.0-6.9)	473	46.7%
Basse (0.1-3.9)	43	4.2%
Indicatori di Rischio		
KEV (Exploit Attivi)	11	0.9%
EPSS Elevato (>50%)	3	0.2%

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

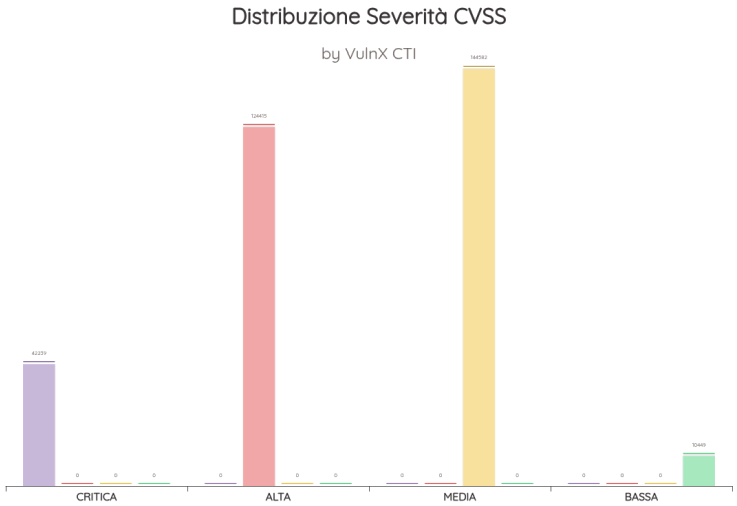
1.2 Panoramica Database (Storico Completo)

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

- **CVE Totali nel Database:** 332,932
- **KEV Totali (Vulnerabilità con Exploit Noti):** 1,520
- **CWE Totali Catalogate:** 969
- **CPE Totali Monitorati:** 2,194,603

Severità	Conteggio	Percentuale
CRITICA	42,239	13.1%
ALTA	124,415	38.7%
MEDIA	144,582	44.9%
BASSA	10,449	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:

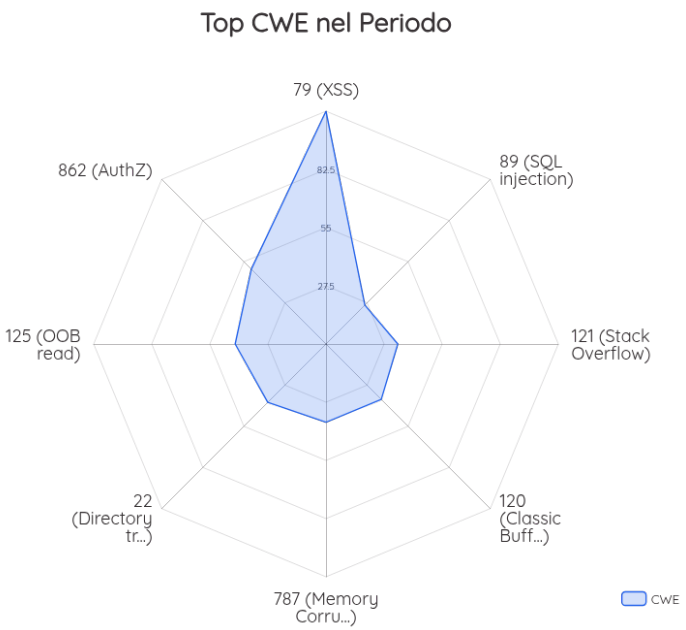


Figura 1: *Distribuzione Top CWE - Grafico Radar*

3.2 Analisi Approfondita delle Debolezze (CWE)

Le debolezze più comuni con raccomandazioni di difesa.

79

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

▶ **Occorrenze:** 110

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per mitigare la CWE-79 (Cross-site Scripting):
- N/A**Implementare l'Output Encoding Contestuale:**Codificare sempre tutti i dati forniti dall'utente prima di renderizzarli nella pagina web, utilizzando funzioni di encoding specifiche per il contesto (es. HTML entity encoding per il testo, URL encoding per gli attributi URL, JavaScript encoding per i blocchi script). Utilizzare librerie di sanitizzazione sicure e aggiornate.
- N/A**Applicare una Validazione Rigorosa dell'Input:**Validare tutti gli input utente sul lato server, verificando il tipo di dato, il formato, la lunghezza massima e l'assenza di caratteri speciali non consentiti, prima di elaborare o memorizzare qualsiasi informazione.
- N/A**Configurare una Content Security Policy (CSP) Robusta:**Implementare una CSP che limiti le fonti da cui il browser può caricare script, stili e altre risorse. Questo riduce significativamente la capacità di un attaccante di eseguire codice malevolo anche in caso di iniezione di script.

862

Missing Authorization

- **Occorrenze:** 50

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per mitigare la debolezza CWE-862 (Missing Authorization):
- N/A**Implementare controlli di autorizzazione espliciti e granulari a livello di codice**per ogni endpoint API e ogni funzione dell'applicazione che gestisce dati sensibili o operazioni privilegiate, verificando i permessi dell'utente prima di concedere l'accesso.
- N/A**Adottare e configurare un framework di autorizzazione robusto**(es. Spring Security per Java, ASP.NET Identity per .NET) per gestire ruoli e permessi in modo centralizzato e coerente attraverso l'intera applicazione.
- N/A**Utilizzare un API Gateway o un Reverse Proxy per imporre controlli di autorizzazione iniziali**(es. validazione token JWT, verifica scope) prima che le richieste raggiungano i servizi backend, fungendo da primo strato di difesa.

121

Stack-based Buffer Overflow

- **Occorrenze:** 34

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-121 - Stack-based Buffer Overflow:
- N/A**Adottare pratiche di codifica sicura:**Utilizzare funzioni per la gestione delle stringhe e della memoria che prevedano sempre il controllo dei limiti (es. ‘snprintf‘, ‘strncpy‘ con dimensione specificata) ed evitare funzioni insicure (es. ‘strcpy‘, ‘sprintf‘, ‘gets‘) che non verificano i confini del buffer.
- N/A**Abilitare le protezioni del compilatore e del sistema operativo:**Configurare i compilatori per abilitare protezioni come Stack Canaries (SSP/GS) e compilare le applicazioni con ASLR (Address Space Layout Randomization) e DEP/NX (Data Execution Prevention/No-Execute) attivi per mitigare l’impatto degli overflow.
- N/A**Integrare SAST e DAST nel ciclo di sviluppo:**Utilizzare strumenti di Static Application Security Testing (SAST) e Dynamic Application Security Testing (DAST) per identificare e correggere proattivamente le vulnerabilità di buffer overflow nel codice sorgente e in fase di runtime.

119

Improper Restriction of Operations within the Bounds of a Memory Buffer

- **Occorrenze:** 22

Raccomandazioni di Difesa

- Ecco 2-3 raccomandazioni di difesa specifiche e attuabili per CWE-119:
- N/A**Implementare una rigorosa validazione degli input:**A livello applicativo e/o tramite WAF (Web Application Firewall), validare sempre la lunghezza e il formato di tutti gli input utente prima di elaborarli, per prevenire l'invio di dati eccessivi o malevoli che potrebbero causare un overflow.
- N/A**Adottare pratiche di sviluppo con gestione sicura della memoria:**Utilizzare funzioni e librerie che gestiscono la memoria in modo sicuro (es. 'strncpy_s', 'snprintf', 'std::string' in C++), evitando API insicure come 'strcpy', 'strcat' o 'sprintf' che non eseguono controlli sui limiti del buffer.
- N/A**Abilitare le protezioni a livello di compilatore e sistema operativo:**Configurare le opzioni del compilatore per abilitare protezioni come Stack Canaries ('-fstack-protector' per GCC/Clang) e assicurarsi che le funzionalità del sistema operativo come ASLR (Address Space Layout Randomization) e DEP/NX (Data Execution Prevention/No-Execute) siano attive per rendere più difficile l'exploit di eventuali buffer overflow.

269

Improper Privilege Management

- **Occorrenze:** 10

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per CWE-269 - Improper Privilege Management:
- N/A**Implementare un modello di controllo degli accessi basato sui ruoli (RBAC) per applicare il principio del privilegio minimo**, assegnando agli utenti e ai servizi solo le autorizzazioni strettamente necessarie per svolgere le proprie funzioni.
- N/A**Adottare una soluzione di Privileged Access Management (PAM)**per gestire, monitorare e registrare l'accesso agli account privilegiati (es. amministratori, root), garantendo la rotazione automatica delle credenziali e sessioni controllate.
- N/A**Implementare processi di revisione e audit regolari (almeno trimestrali) dei permessi e dei ruoli**assegnati a utenti, gruppi e servizi. Revocare immediatamente i privilegi non più necessari o eccessivi.

617

Reachable Assertion

- **Occorrenze:** 5

Raccomandazioni di Difesa

- Ecco 2-3 raccomandazioni specifiche e attuabili per mitigare la debolezza CWE-617 (Reachable Assertion):
- N/A**Pratiche di Sviluppo:**Eliminare tutte le istruzioni di asserzione (assertions) dal codice destinato agli ambienti di produzione. Le asserzioni dovrebbero essere utilizzate esclusivamente per il debugging e i test in fase di sviluppo.
- N/A**Configurazioni di Build:**Implementare e far rispettare l'uso di configurazioni di build distinte (ad esempio, "release" vs "debug") che rimuovano automaticamente o disabilitino le asserzioni quando il codice viene compilato per il deployment in produzione.
- N/A**Gestione degli Errori:**Assicurarsi che qualsiasi output generato da un'asserzione (qualora una dovesse rimanere e venire attivata) non sia mai esposto agli utenti finali. Implementare una gestione degli errori robusta che registri internamente tali eventi (logging sicuro) e presenti all'utente solo messaggi di errore generici e non informativi.

3.3 CVE del Periodo Analizzato

Trovate **1242** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **25** CVE:

CVE-2026-1490 - CVSS 9.8 (CRITICA)

Il plugin Spam protection, Anti-Spam, FireWall di CleanTalk per WordPress è vulnerabile a installazioni arbitrarie di plugin non autorizzate a causa di un bypass dell'autorizzazione tramite spoofing del record reverse DNS (PTR) sulla funzione 'checkWithoutToken' in tutte le versioni fino alla 6.71 inclusa. Ciò rende possibile a attaccanti non autenticati installare e attivare plugin arbitrari, che possono essere sfruttati per ottenere l'esecuzione di codice remoto se un altro plugin vulnerabile è installato e attivato. Nota: Questa vulnerabilità è sfruttabile solo su siti con una chiave API non valida.

Descrizione Originale (EN): The Spam protection, Anti-Spam, FireWall by CleanTalk plugin for WordPress is vulnerable to unauthorized Arbitrary Plugin Installation due to an authorization bypass via reverse DNS (PTR record) spoofing on the 'checkWithoutToken' function in all versions up to, and including, 6.71. This makes it possible for unauthenticated attackers to install and activate arbitrary plugins which can be leveraged to achieve remote code execution if another vulnerable plugin is installed and activated. Note: This is only exploitable on sites with an invalid API key.

Cosa può succedere?
Un attaccante non autenticato può ottenere il controllo completo del sito WordPress, permettendo il furto di dati sensibili, l'interruzione dei servizi o l'installazione di malware. Ciò può portare a gravi perdite finanziarie e danni alla reputazione aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.08% (Percentile: 0.24)
Pubblicata:	15/02/2026
Modificata:	15/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Applica permessi di scrittura restrittivi alla directory 'wp-content/plugins' e ad altre directory sensibili del tuo ambiente WordPress. Consenti la scrittura solo durante gli aggiornamenti o le installazioni di plugin autorizzate, impedendo così agli attaccanti non autenticati di installare e attivare 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

350: **Reliance on Reverse DNS Resolution for a Security-Critical Action**

Approfondisci su VulnX

CVE-2026-26366 - CVSS 9.8 (CRITICA)

eNet SMART HOME server 2.2.1 e 2.3.1 vengono forniti con credenziali di default (user:user, admin:admin) che rimangono attive dopo l'installazione e la messa in servizio senza imporre un cambio password obbligatorio. Gli attaccanti non autenticati possono utilizzare queste credenziali di default per ottenere accesso amministrativo a funzioni sensibili di configurazione e controllo della smart home.

Descrizione Originale (EN): eNet SMART HOME server 2.2.1 and 2.3.1 ships with default credentials (user:user, admin:admin) that remain active after installation and commissioning without enforcing a mandatory password change. Unauthenticated attackers can use these default credentials to gain administrative access to sensitive smart home configuration and control functions.

Cosa può succedere?

Gli aggressori possono ottenere il pieno controllo del sistema eNet SMART HOME, consentendo l'accesso non autorizzato alle proprietà fisiche e la manipolazione delle funzioni di sicurezza e controllo ambientale. Ciò potrebbe portare a gravi violazioni della sicurezza, interruzioni operative e potenziali danni alla reputazione aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	15/02/2026
Modificata:	15/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare il server eNet SMART HOME in una VLAN di rete dedicata e strettamente segmentata. Bloccare qualsiasi accesso dall'esterno (Internet) e limitare le connessioni in ingresso solo ai dispositivi o utenti interni strettamente necessari per la sua operatività, riducendo drasticamente la superficie d'attacco sfruttabile tramite le credenziali di default.

CVSS Metrics

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

CWE - Common Weakness Enumeration

1392: **Use of Default Credentials**

Approfondisci su VulnX

CVE-2025-32058 - CVSS 9.3 (CRITICA)

L'ECU di Infotainment prodotto da Bosch utilizza un modulo RH850 per la comunicazione CAN. RH850 è collegato all'infotainment tramite l'interfaccia INC attraverso un protocollo personalizzato. Esiste una vulnerabilità durante l'elaborazione delle richieste di questo protocollo sul lato V850 che consente a un attaccante con esecuzione di codice sul SoC principale dell'infotainment di eseguire codice sul modulo RH850 e successivamente inviare messaggi CAN arbitrari sulla rete CAN collegata. Identificata per la prima volta su Nissan Leaf ZE1 prodotta nel 2020.

Descrizione Originale (EN): The Infotainment ECU manufactured by Bosch uses a RH850 module for CAN communication. RH850 is connected to infotainment over the INC interface through a custom protocol. There is a vulnerability during processing requests of this protocol on the V850 side which allows an attacker with code execution on the infotainment main SoC to perform code execution on the RH850 module and subsequently send arbitrary CAN messages over the connected CAN bus. First identified on Nissan Leaf ZE1 manufactured in 2020.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo dei sistemi critici del veicolo. Ciò potrebbe causare gravi interruzioni del servizio, malfunzionamenti critici o persino incidenti, con conseguenti danni reputazionali e finanziari significativi per l'azienda.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	0.01% (Percentile: 0.02)
Pubblicata:	15/02/2026
Modificata:	15/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Dato che l'attacco sfrutta una pre-esistente esecuzione di codice sul SoC principale dell'infotainment, è cruciale implementare una rigorosa segmentazione della rete per isolare questo sistema da altre reti veicolari critiche e da accessi esterni non autorizzati. Restringere e monitorare attentamente tutti i punti di accesso e le comunicazioni in entrata/uscita del sistema di infotainment per prevenire una compromissione iniziale del SoC.

CVSS Metrics

- **Vettore di Attacco:** local
- **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

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2025-32061 - CVSS 8.8 (ALTA)

Il difetto specifico si trova all'interno dello stack Bluetooth sviluppato da Alps Alpine dell'ECU Infotainment prodotto da Bosch. Il problema deriva dalla mancanza di una corretta convalida dei limiti dei dati forniti dall'utente, che può causare un overflow del buffer basato su stack durante la ricezione di un pacchetto specifico sul canale L2CAP di livello superiore stabilito. Un attaccante può sfruttare questa vulnerabilità per ottenere l'esecuzione di codice remoto sull'ECU Infotainment con privilegi di root. Identificato per la prima volta su Nissan Leaf ZE1 prodotta nel 2020.

Descrizione Originale (EN): The specific flaw exists within the Bluetooth stack developed by Alps Alpine of the Infotainment ECU manufactured by Bosch. The issue results from the lack of proper boundary validation of user-supplied data, which can result in a stack-based buffer overflow when receiving a specific packet on the established upper layer L2CAP channel. An attacker can leverage this vulnerability to obtain remote code execution on the Infotainment ECU with root privileges. First identified on Nissan Leaf ZE1 manufactured in 2020.

Cosa può succedere?
Un attaccante potrebbe ottenere il controllo completo del sistema di infotainment del veicolo. Ciò potrebbe comportare il furto di dati sensibili degli utenti, l'interruzione dei servizi del veicolo e potenzialmente la compromissione della sicurezza generale del mezzo.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.04% (Percentile: 0.12)
Pubblicata:	15/02/2026
Modificata:	15/02/2026
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 di infotainment dalle reti di controllo critiche del veicolo. Questo limita la capacità di un attaccante di spostarsi lateralmente da un'unità infotainment compromessa a sistemi più critici, contenendo il raggio d'azione della vulnerabilità.

CVSS Metrics

- **Vettore di Attacco:** adjacent_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

Approfondisci su VulnX

CVE-2025-32062 - CVSS 8.8 (ALTA)

Il difetto specifico si trova all'interno dello stack Bluetooth sviluppato da Alps Alpine dell'ECU Infotainment prodotto da Bosch. Il problema deriva dalla mancanza di una corretta convalida dei limiti dei dati forniti dall'utente, che può causare un overflow del buffer basato su stack durante la ricezione di un pacchetto specifico sul canale L2CAP di livello superiore stabilito. Un attaccante può sfruttare questa vulnerabilità per ottenere l'esecuzione di codice remoto sull'ECU Infotainment con privilegi di root. Identificato per la prima volta su Nissan Leaf ZE1 prodotta nel 2020.

Descrizione Originale (EN): The specific flaw exists within the Bluetooth stack developed by Alps Alpine of the Infotainment ECU manufactured by Bosch. The issue results from the lack of proper boundary validation of user-supplied data, which can result in a stack-based buffer overflow when receiving a specific packet on the established upper layer L2CAP channel. An attacker can leverage this vulnerability to obtain remote code execution on the Infotainment ECU with root privileges. First identified on Nissan Leaf ZE1 manufactured in 2020.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo remoto completo del sistema di infotainment del veicolo. Questo permetterebbe il furto di dati sensibili degli utenti o la manipolazione delle funzionalità del sistema, causando interruzioni operative e potenziali rischi per la privacy.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.04% (Percentile: 0.12)
Pubblicata:	15/02/2026
Modificata:	15/02/2026
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 i sistemi di gestione e diagnostica che interagiscono con le ECU Infotainment vulnerabili in una rete segmentata dedicata. Implementare rigorose regole firewall per limitare la comunicazione esclusivamente ai protocolli essenziali e a fonti attendibili, contenendo così il potenziale impatto di una compromissione.

CVSS Metrics

- **Vettore di Attacco:** adjacent_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

Approfondisci su VulnX

CVE-2025-32059 - CVSS 8.8 (ALTA)

Il difetto specifico si trova all'interno dello stack Bluetooth sviluppato da Alps Alpine dell'ECU Infotainment prodotto da Bosch. Il problema deriva dalla mancanza di una corretta convalida dei limiti dei dati forniti dall'utente, che può causare un overflow del buffer basato su stack durante la ricezione di un pacchetto specifico sul canale L2CAP di livello superiore stabilito. Un attaccante può sfruttare questa vulnerabilità per ottenere l'esecuzione di codice remoto sull'ECU Infotainment con privilegi di root. Identificato per la prima volta su Nissan Leaf ZE1 prodotta nel 2020.

Descrizione Originale (EN): The specific flaw exists within the Bluetooth stack developed by Alps Alpine of the Infotainment ECU manufactured by Bosch. The issue results from the lack of proper boundary validation of user-supplied data, which can result in a stack-based buffer overflow when receiving a specific packet on the established upper layer L2CAP channel. An attacker can leverage this vulnerability to obtain remote code execution on the Infotainment ECU with root privileges. First identified on Nissan Leaf ZE1 manufactured in 2020.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo remoto completo dell'unità di infotainment del veicolo. Questo permetterebbe di accedere a dati sensibili degli utenti o di manipolare le funzionalità del veicolo. Le conseguenze includono interruzioni operative, gravi rischi per la sicurezza e danni alla reputazione aziendale.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	0.04% (Percentile: 0.12)
Pubblicata:	15/02/2026
Modificata:	15/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Fino alla disponibilità di una patch, disabilitare la funzionalità Bluetooth sugli ECU Infotainment quando non è strettamente necessaria per le operazioni critiche. Implementare politiche di sicurezza che prevedano l'attivazione del Bluetooth solo su richiesta e per periodi limitati, riducendo proattivamente la superficie di attacco e l'esposizione a questa vulnerabilità.

CVSS Metrics

- **Vettore di Attacco:** adjacent_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

Approfondisci su VulnX

CVE-2026-26333 - CVSS 10.0 (CRITICA)

Le versioni di Calero VeraSMART precedenti alla 2022 R1 espongono un servizio HTTP .NET Remoting non autenticato sulla porta TCP 8001. Il servizio pubblica ObjectURIs predefiniti (tra cui EndeavorServer.rem e RemoteFileReceiver.rem) e consente l'uso di SOAP e formatter binari con TypeFilterLevel impostato su Full. Un attaccante remoto non autenticato può invocare gli endpoint remoti esposti per eseguire operazioni arbitrarie di lettura e scrittura di file tramite la classe WebClient. Ciò permette di recuperare file sensibili come WebRoot\{}\{}web.config, che può divulgare le chiavi di validazione e decrittazione machineKey di IIS. Un attaccante può utilizzare queste chiavi per generare un payload malicious di ASP.NET ViewState e ottenere l'esecuzione di codice remoto nel contesto dell'applicazione IIS. Inoltre, fornendo un percorso UNC, è possibile innescare un'autenticazione SMB in uscita dal account di servizio, potenzialmente esponendo hash NTLMv2 per relaying o cracking offline.

Descrizione Originale (EN): Calero VeraSMART versions prior to 2022 R1 expose an unauthenticated .NET Remoting HTTP service on TCP port 8001. The service publishes default ObjectURIs (including EndeavorServer.rem and RemoteFileReceiver.rem) and permits the use of SOAP and binary formatters with TypeFilterLevel set to Full. An unauthenticated remote attacker can invoke the exposed remoting endpoints to perform arbitrary file read and write operations via the WebClient class. This allows retrieval of sensitive files such as WebRoot\{}\{}web.config, which may disclose IIS machineKey validation and decryption keys. An attacker can use these keys to generate a malicious ASP.NET ViewState payload and achieve remote code execution within the IIS application context. Additionally, supplying a UNC path can trigger outbound SMB authentication from the service account, potentially exposing NTLMv2 hashes for relay or offline cracking.

Cosa può succedere?

Un aggressore remoto non autenticato può ottenere il controllo completo dei sistemi aziendali vulnerabili. Questo permetterebbe il furto di dati sensibili, la manipolazione o la cancellazione di informazioni critiche, e la potenziale interruzione dei servizi essenziali dell'azienda.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.10% (Percentile: 0.27) Disponibili 2 valori storici
Pubblicata:	13/02/2026
Modificata:	13/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Isolare immediatamente i sistemi Calero VeraSMART che espongono il servizio vulnerabile in una zona di rete altamente segmentata. Implementare regole firewall per bloccare tutto il traffico in entrata verso la porta TCP 8001, consentendo l'accesso solo da indirizzi IP o reti strettamente autorizzate e indispensabili per la funzionalità del servizio.

CVSS Metrics

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

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

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-2026-26221 - CVSS 10.0 (CRITICA)

Hyland OnBase presenta un'esposizione non autenticata di .NET Remoting nel servizio OnBase Workflow Timer Service (Hyland.Core.Workflow.NTService.exe). Un attaccante in grado di raggiungere il servizio può inviare richieste .NET Remoting manipolate agli endpoint del canale HTTP predefinito su TCP/8900 (ad esempio, TimerServiceAPI.rem e TimerServiceEvents.rem per Workflow) per innescare il deserializzazione di oggetti non sicura, consentendo la lettura/scrittura arbitraria di file. Scrivendo contenuti controllati dall'attaccante in posizioni accessibili tramite web o combinando questa vulnerabilità con altre funzionalità di OnBase, è possibile ottenere l'esecuzione di codice remoto. Lo stesso primitive può essere sfruttato fornendo un percorso UNC per forzare l'autenticazione outbound NTLM (coercizione SMB) verso un host controllato dall'attaccante.

Descrizione Originale (EN): Hyland OnBase contains an unauthenticated .NET Remoting exposure in the OnBase Workflow Timer Service (Hyland.Core.Workflow.NTService.exe). An attacker who can reach the service can send crafted .NET Remoting requests to default HTTP channel endpoints on TCP/8900 (e.g., TimerServiceAPI.rem and TimerServiceEvents.rem for Workflow) to trigger unsafe object unmarshalling, enabling arbitrary file read/write. By writing attacker-controlled content into web-accessible locations or chaining with other OnBase features, this can lead to remote code execution. The same primitive can be abused by supplying a UNC path to coerce outbound NTLM authentication (SMB coercion) to an attacker-controlled host.

Cosa può succedere?

Un attaccante non autenticato può ottenere il controllo completo del server OnBase, consentendo la lettura, la modifica o la cancellazione di dati sensibili e file di sistema. Ciò può portare a gravi interruzioni dei servizi aziendali, al furto di informazioni riservate e alla potenziale compromissione dell'intera rete aziendale.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.52% (Percentile: 0.66) Disponibili 2 valori storici
Pubblicata:	13/02/2026
Modificata:	13/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare immediatamente una rigorosa segmentazione di rete per il servizio OnBase Workflow Timer Service (Hyland.Core.Workflow.NTService.exe). Configurare regole firewall per limitare l'accesso alla porta TCP/8900 esclusivamente ai sistemi interni e agli utenti strettamente necessari, isolandola da reti non affidabili e da Internet. Questo ridurrà drasticamente la superficie d'attacco e la raggiungibilità del servizio vulnerabile.

CVSS Metrics

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

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-2025-69770 - CVSS 10.0 (CRITICA)

Una vulnerabilità zip slip nell'endpoint /DesignTools/SkinList.aspx di MojoPortal CMS v2.9.0.1 consente agli attacker di eseguire comandi arbitrari tramite l'upload di un file zip manipolato.

Descrizione Originale (EN): A zip slip vulnerability in the /DesignTools/SkinList.aspx endpoint of MojoPortal CMS v2.9.0.1 allows attackers to execute arbitrary commands via uploading a crafted zip file.

Cosa può succedere?

Gli attaccanti possono ottenere il controllo completo dei sistemi aziendali, consentendo il furto di dati critici, la totale interruzione dei servizi web e l'installazione di software malevolo (es. ransomware). Questo può portare a gravi perdite finanziarie e danni alla reputazione aziendale.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.09% (Percentile: 0.25) Disponibili 2 valori storici
Pubblicata:	13/02/2026
Modificata:	13/02/2026
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 esecuzione di comandi arbitrari, configurare il server web che ospita MojoPortal con il principio del minimo privilegio, assicurando che l'account di servizio non abbia permessi di scrittura su directory di sistema o di esecuzione di binari non essenziali. Parallelamente, implementare un monitoraggio avanzato dell'integrità dei file (FIM) sulle directory critiche del sistema e dell'applicazione per rilevare immediatamente modifiche non autorizzate.

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

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

Probabilità di Sfruttamento: high

Termini Alternativi: Directory traversal, Path traversal

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-26216 - CVSS 10.0 (CRITICA)

Crawl4AI versioni precedenti alla 0.8.0 presentano una vulnerabilità di esecuzione remota di codice nell'implementazione dell'API Docker. L'endpoint /crawl accetta un parametro hooks contenente codice Python che viene eseguito tramite exec(). Il builtin __import__ era incluso tra i builtins consentiti, consentendo agli attaccanti remoti non autenticati di importare moduli arbitrari ed eseguire comandi di sistema. Un exploitation riuscito permette la compromissione completa del server, inclusa l'esecuzione arbitraria di comandi, accesso in lettura e scrittura ai file, esfiltrazione di dati sensibili e movimento laterale all'interno delle reti interne.

Descrizione Originale (EN): Crawl4AI versions prior to 0.8.0 contain a remote code execution vulnerability in the Docker API deployment. The /crawl endpoint accepts a hooks parameter containing Python code that is executed using exec(). The __import__ builtin was included in the allowed builtins, allowing unauthenticated remote attackers to import arbitrary modules and execute system commands. Successful exploitation allows full server compromise, including arbitrary command execution, file read and write access, sensitive data exfiltration, and lateral movement within internal networks.

Cosa può succedere?
Un attaccante può ottenere il controllo completo del server, rubare dati sens sensibili e interrompere i servizi critici senza autenticazione. Questo può causare gravi perdite finanziarie, danni alla reputazione e interruzioni operative prolungate.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	0.20% (Percentile: 0.42) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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 Crawl4AI in un segmento di rete dedicato o una DMZ e applicare rigorose regole di firewall. Limitare l'accesso all'endpoint '/crawl' esclusivamente a indirizzi IP o host interni specifici e autorizzati, impedendo così agli attaccanti remoti non autenticati di raggiungere la superficie vulnerabile.

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-2026-26369 - CVSS 9.8 (CRITICA)

eNet SMART HOME server 2.2.1 e 2.3.1 contengono una vulnerabilità di escalation dei privilegi dovuta a controlli di autorizzazione insufficienti nel metodo setUserGroup JSON-RPC. Un utente con privilegi bassi (UG_USER) può inviare una richiesta POST manipolata a /jsonrpc/management specificando il proprio nome utente per elevare il proprio account al gruppo UG_ADMIN, bypassando i controlli di accesso previsti e ottenendo capacità amministrative come la modifica delle configurazioni dei dispositivi, le impostazioni di rete e altre funzioni del sistema smart home.

Descrizione Originale (EN): eNet SMART HOME server 2.2.1 and 2.3.1 contains a privilege escalation vulnerability due to insufficient authorization checks in the setUserGroup JSON-RPC method. A low-privileged user (UG_USER) can send a crafted POST request to /jsonrpc/management specifying their own username to elevate their account to the UG_ADMIN group, bypassing intended access controls and gaining administrative capabilities such as modifying device configurations, network settings, and other smart home system functions.

Cosa può succedere?
Un utente con privilegi bassi potrebbe ottenere il controllo amministrativo completo del sistema eNet SMART HOME. Questo permetterebbe di manipolare le configurazioni dei dispositivi, causando gravi interruzioni operative, compromettendo la sicurezza fisica degli ambienti e consentendo accessi non autorizzati a funzioni critiche.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	15/02/2026
Modificata:	15/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
In assenza di una patch, implementare un Web Application Firewall (WAF) o un reverse proxy davanti al server eNet SMART HOME. Configurare il WAF/proxy per ispezionare e bloccare le richieste POST manipolate dirette a '/jsonrpc/management' che tentano di modificare i privilegi utente, impedendo l'escalation a UG_ADMIN.

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-2025-8572 - CVSS 9.8 (CRITICA)

Il plugin Truelysell Core per WordPress è vulnerabile a escalation dei privilegi nelle versioni inferiori o uguali a 1.8.7. Ciò è dovuto a una validazione insufficiente del parametro user_role durante la registrazione dell'utente. Questo rende possibile agli attori malevoli non autenticati creare account con privilegi elevati, inclusi accessi da amministratore.

Descrizione Originale (EN): The Truelysell Core plugin for WordPress is vulnerable to privilege escalation in versions less than, or equal to, 1.8.7. This is due to insufficient validation of the user_role parameter during user registration. This makes it possible for unauthenticated attackers to create accounts with elevated privileges, including administrator access.

Cosa può succedere?

Attaccanti non autenticati potrebbero ottenere pieno controllo amministrativo del sito web. Ciò consentirebbe il furto di dati sensibili (es. informazioni clienti), la manipolazione dei contenuti, l'iniezione di codice malevolo o la completa interruzione dei servizi, con gravi conseguenze finanziarie e reputazionali per l'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 2 valori storici
Pubblicata:	14/02/2026
Modificata:	14/02/2026
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 monte dell'istanza WordPress. Configurare il WAF per ispezionare le richieste di registrazione utente e bloccare quelle che tentano di manipolare il parametro 'user_role' o che indicano la creazione di account con privilegi elevati. Questo agirà come controllo compensativo per prevenire l'escalation dei privilegi 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

269: **Improper Privilege Management**

Probabilità di Sfruttamento: medium

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-1306 - CVSS 9.8 (CRITICA)

Il plugin midi-Synth per WordPress è vulnerabile a caricamenti arbitrari di file a causa della mancanza di validazione del tipo di file e dell'estensione del file nell'azione AJAX 'export' in tutte le versioni fino alla 1.1.0 inclusa. Ciò rende possibile agli attaccanti non autenticati caricare file arbitrari sul server del sito interessato, il che potrebbe consentire l'esecuzione di codice remoto, a condizione che l'attaccante possa ottenere un nonce valido. Il nonce è esposto nel JavaScript frontend, rendendolo facilmente accessibile agli attaccanti non autenticati.

Descrizione Originale (EN): The midi-Synth plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type and file extension validation in the 'export' AJAX action in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible granted the attacker can obtain a valid nonce. The nonce is exposed in frontend JavaScript making it trivially accessible to unauthenticated attackers.

Cosa può succedere?

Un attaccante potrebbe caricare file malevoli sul server, ottenendo il controllo completo del sito web e del server. Ciò consentirebbe il furto di dati sensibili, l'interruzione dei servizi o l'utilizzo della piattaforma compromessa per lanciare ulteriori attacchi.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.14% (Percentile: 0.34) Disponibili 2 valori storici
Pubblicata:	14/02/2026
Modificata:	14/02/2026
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) per monitorare e filtrare il traffico HTTP/S diretto al server WordPress. Configurare il WAF per bloccare tentativi di caricamento di file con estensioni o tipi MIME sospetti (es. .php, .exe) in directory non previste, mitigando così il rischio di esecuzione di codice remoto tramite upload arbitrari.

CVSS Metrics

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

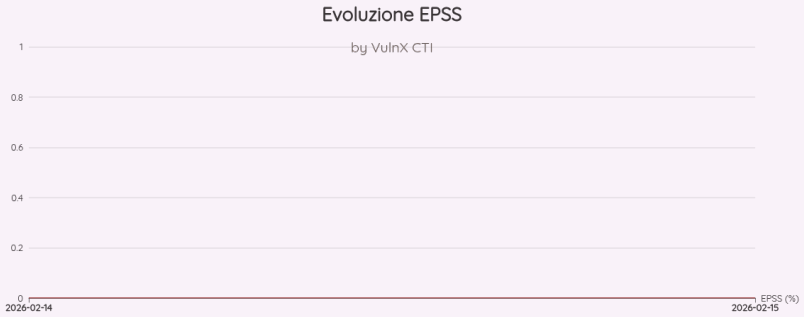
CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Unrestricted File Upload

Evoluzione EPSS nel Tempo:



Approfondisci su VulnX

CVE-2026-26273 - CVSS 9.8 (CRITICA)

Known è una piattaforma di social publishing. Prima di 1.6.3, esiste una vulnerabilità critica di Broken Authentication in Known 1.6.2 e versioni precedenti. L'applicazione rivela il token di reset della password all'interno di un campo HTML nascosto sulla pagina di reset della password. Ciò consente a qualsiasi attaccante non autenticato di recuperare il token di reset di qualsiasi utente semplicemente interrogando l'indirizzo email dell'utente, portando a un completo Account Takeover (ATO) senza richiedere l'accesso alla casella di posta elettronica della vittima. Questa vulnerabilità è stata corretta in 1.6.3.

Descrizione Originale (EN): Known is a social publishing platform. Prior to 1.6.3, a Critical Broken Authentication vulnerability exists in Known 1.6.2 and earlier. The application leaks the password reset token within a hidden HTML input field on the password reset page. This allows any unauthenticated attacker to retrieve the reset token for any user by simply querying the user's email, leading to full Account Takeover (ATO) without requiring access to the victim's email inbox. This vulnerability is fixed in 1.6.3.

Cosa può succedere?

Un attaccante non autenticato potrebbe assumere il controllo completo di qualsiasi account utente sulla piattaforma. Questo permetterebbe il furto di dati sensibili, la manipolazione o cancellazione di contenuti, e l'invio di informazioni dannose, causando gravi danni alla reputazione aziendale e potenziali interruzioni dei servizi.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.08% (Percentile: 0.24) Disponibili 2 valori storici
Pubblicata:	13/02/2026
Modificata:	13/02/2026
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 monte dell'applicazione Known. Configurare il WAF per ispezionare e modificare le risposte HTTP della pagina di reset della password, rimuovendo o oscurando il campo HTML nascosto che espone il token di reset. Questa misura infrastrutturale fungerà da controllo compensativo essenziale per prevenire l'abuso 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

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

Probabilità di Sfruttamento: high

Termini Alternativi: Information Disclosure, Information Leak

---

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

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-26190 - CVSS 9.8 (CRITICA)

Milvus è un database vettoriale open-source progettato per applicazioni di generative AI. Prima delle versioni 2.5.27 e 2.6.10, Milvus espone di default la porta TCP 9091, il che consente bypass di autenticazione. L'endpoint di debug /expr utilizza un token di autenticazione predefinito debole e prevedibile, derivato da etcd.rootPath (predefinito: by-dev), che permette la valutazione arbitraria di espressioni. L'intera API REST (/api/v1/*) è registrata sulla porta metrics/management senza alcuna autenticazione, consentendo l'accesso non autenticato a tutte le operazioni di business, inclusa la manipolazione dei dati e la gestione delle credenziali. Questa vulnerabilità è stata corretta nelle versioni 2.5.27 e 2.6.10.

Descrizione Originale (EN): Milvus is an open-source vector database built for generative AI applications. Prior to 2.5.27 and 2.6.10, Milvus exposes TCP port 9091 by default, which enables authentication bypasses. The /expr debug endpoint uses a weak, predictable default authentication token derived from etcd.rootPath (default: by-dev), enabling arbitrary expression evaluation. The full REST API (/api/v1/*) is registered on the metrics/management port without any authentication, allowing unauthenticated access to all business operations including data manipulation and credential management. This vulnerability is fixed in 2.5.27 and 2.6.10.

Cosa può succedere?

Un attaccante potrebbe accedere senza autenticazione al database Milvus, rubando o manipolando dati sensibili utilizzati dalle applicazioni di intelligenza artificiale generativa. Ciò potrebbe compromettere l'integrità dei modelli AI, causare interruzioni del servizio e potenzialmente consentire l'esecuzione di comandi arbitrari sul sistema.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.11% (Percentile: 0.29) Disponibili 2 valori storici
Pubblicata:	13/02/2026
Modificata:	13/02/2026
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 le istanze Milvus. Configurare i firewall perimetrali e host-based per bloccare tutte le connessioni in ingresso alla porta TCP 9091 da reti non fidate, consentendo l'accesso solo da host o servizi interni specifici e autorizzati che ne necessitano assolutamente. Ciò riduce significativamente la superficie di attacco limitando l'esposizione dell'endpoint di debug vulnerabile.

CVSS Metrics

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

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2019-25337 - CVSS 9.8 (CRITICA)

OwnCloud 8.1.8 presenta una vulnerabilità di enumerazione degli username che consente agli attaccanti remoti di scoprire account utente manipolando l'endpoint share.php. Gli aggressori possono inviare richieste GET appositamente formulate a /index.php/core/ajax/share.php con un parametro di ricerca con carattere jolly per ottenere informazioni complete sugli utenti.

Descrizione Originale (EN): OwnCloud 8.1.8 contains a username enumeration vulnerability that allows remote attackers to discover user accounts by manipulating the share.php endpoint. Attackers can send crafted GET requests to /index.php/core/ajax/share.php with a wildcard search parameter to retrieve comprehensive user information.

Cosa può succedere?
Gli aggressori possono facilmente scoprire i nomi utente validi, facilitando attacchi di forza bruta e campagne di phishing mirate. Ciò può portare all'accesso non autorizzato ai dati aziendali, al furto di informazioni sensibili e alla potenziale compromissione del sistema.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.11% (Percentile: 0.30) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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, implementare un Web Application Firewall (WAF) o configurare il reverse proxy per ispezionare e limitare le richieste all'endpoint '/index.php/core/ajax/share.php'. Definire regole specifiche per bloccare richieste con caratteri jolly o volumi anomali, impedendo così l'enumerazione degli account utente.

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

203: **Observable Discrepancy**

Termini Alternativi: Side Channel Attack

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2019-25321 - CVSS 9.8 (CRITICA)

FTP Navigator 8.03 presenta una vulnerabilità di overflow dello stack che consente agli attaccanti di eseguire codice arbitrario sovrascrivendo i registri Structured Exception Handler (SEH). Gli attaccanti possono creare una payload dannosa che attiva un overflow del buffer quando incollata nel campo di testo Custom Command, consentendo l'esecuzione di codice remoto e il lancio della calcolatrice come prova di concetto.

Descrizione Originale (EN): FTP Navigator 8.03 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload that triggers a buffer overflow when pasted into the Custom Command textbox, enabling remote code execution and launching the calculator as proof of concept.

Cosa può succedere?

Sfruttando questa vulnerabilità, un attaccante potrebbe ottenere il controllo completo del sistema affetto. Ciò consentirebbe il furto di dati sensibili, l'interruzione delle operazioni aziendali o l'installazione di software dannoso, come ransomware.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.18% (Percentile: 0.39) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare tutti i sistemi che eseguono FTP Navigator 8.03 in una rete segmentata dedicata. Applicare regole di firewall restrittive per limitare la comunicazione in ingresso e in uscita da questi sistemi, minimizzando la superficie di attacco e il potenziale raggio d'azione in caso di compromissione.

CVSS Metrics

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

CWE - Common Weakness Enumeration

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2019-25319 - CVSS 9.8 (CRITICA)

Domain Quester Pro 6.02 presenta una vulnerabilità di overflow dello stack che consente agli attaccanti remoti di eseguire codice arbitrario sovrascrivendo i registri Structured Exception Handler (SEH). Gli attaccanti possono creare un payload dannoso mirato al campo di input 'Domain Name Keywords' per innescare una violazione di accesso ed eseguire una shell bind sulla porta 9999.

Descrizione Originale (EN): Domain Quester Pro 6.02 contains a stack overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the 'Domain Name Keywords' input field to trigger an access violation and execute a bind shell on port 9999.

Cosa può succedere?

Sfruttando questa vulnerabilità, gli attaccanti potrebbero ottenere il controllo completo del sistema affetto, consentendo il furto di dati sensibili o la manipolazione delle informazioni. Ciò potrebbe portare all'interruzione dei servizi critici, all'installazione di malware o all'utilizzo del sistema compromesso per attaccare altre risorse all'interno della rete aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.18% (Percentile: 0.39) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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 mancanza di patch, isolare il server che esegue Domain Quester Pro 6.02 in un segmento di rete dedicato e altamente ristretto. Implementare rigorose regole di firewall per limitare l'accesso in entrata solo ai servizi essenziali e sorgenti autorizzate, bloccando contestualmente tutte le connessioni in uscita, in particolare verso porte non standard come la 9999, per contenere l'impatto di un'eventuale compromissione.

CVSS Metrics

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

CWE - Common Weakness Enumeration

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2019-25327 - CVSS 9.8 (CRITICA)

Prime95 versione 29.8 build 6 contiene una vulnerabilità di overflow del buffer nel campo di input dell'ID utente che consente agli attaccanti remoti di eseguire codice arbitrario. Gli attaccanti possono creare un payload dannoso e incollarlo nei campi ID utente e proxy host di PrimeNet per attivare una bind shell sulla porta 3110.

Descrizione Originale (EN): Prime95 version 29.8 build 6 contains a buffer overflow vulnerability in the user ID input field that allows remote attackers to execute arbitrary code. Attackers can craft a malicious payload and paste it into the PrimeNet user ID and proxy host fields to trigger a bind shell on port 3110.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo del sistema compromesso, consentendo il furto di dati aziendali sensibili e l'interruzione delle operazioni critiche. Questo comporta gravi rischi per la sicurezza delle informazioni, la continuità del servizio e potenziali perdite finanziarie.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.18% (Percentile: 0.39) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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, isolare immediatamente tutti i sistemi che eseguono Prime95 versione 29.8 build 6 in un segmento di rete dedicato. Implementare rigorose regole di firewalling, sia a livello di rete che sull'host, per bloccare tutte le connessioni in ingresso non autorizzate verso questi sistemi.

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-2026-1358 - CVSS 9.8 (CRITICA)

Airleader Master versioni 6.381 e precedenti consentono il caricamento di file senza restrizioni su più pagine web che funzionano con privilegi massimi. Ciò potrebbe consentire a un utente non autenticato di ottenere potenzialmente l'esecuzione di codice remoto sul server.

Descrizione Originale (EN): Airleader Master versions 6.381 and prior allow for file uploads without restriction to multiple webpages running maximum privileges. This could allow an unauthenticated user to potentially obtain remote code execution on the server.

Cosa può succedere?

Un aggressore non autenticato potrebbe ottenere il controllo completo del server, permettendo il furto di dati sensibili, l'interruzione dei servizi o l'installazione di software dannoso come ransomware. Ciò potrebbe compromettere gravemente la riservatezza, l'integrità e la disponibilità dei sistemi aziendali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.13% (Percentile: 0.33) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolate il server Airleader Master in un segmento di rete dedicato e strettamente controllato (es. DMZ). Implementate regole firewall restrittive per consentire l'accesso all'applicazione solo da indirizzi IP e porte specifici e autorizzati, bloccando ogni accesso non necessario dall'esterno o da segmenti di rete meno affidabili. Ciò ridurrà drasticamente l'esposizione a tentativi di sfruttamento non autenticati e limiterà il potenziale raggio d'azione in caso di compromissione.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Unrestricted File Upload

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2020-37167 - CVSS 9.8 (CRITICA)

L'interprete di bytecode di ClamAV ClamBC presenta una vulnerabilità nella gestione dei nomi delle funzioni che consente agli attaccanti di manipolare i nomi delle funzioni nel bytecode. Gli aggressori possono sfruttare la debole validazione dell'input nell'encoding dei nomi delle funzioni per potenzialmente eseguire bytecode dannoso o causare comportamenti imprevisti nel motore ClamAV.

Descrizione Originale (EN): ClamAV ClamBC bytecode interpreter contains a vulnerability in function name processing that allows attackers to manipulate bytecode function names. Attackers can exploit the weak input validation in function name encoding to potentially execute malicious bytecode or cause unexpected behavior in the ClamAV engine.

Cosa può succedere?

Un aggressore potrebbe eseguire codice malevolo sul sistema dove ClamAV è in funzione, ottenendo il controllo completo. Ciò potrebbe portare al furto di dati sensibili, alla compromissione del sistema o all'interruzione dei servizi aziendali critici.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.03% (Percentile: 0.09) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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 servizi ClamAV in ambienti strettamente segmentati, come container o macchine virtuali dedicate, con privilegi di sistema e di rete minimi. Questo riduce drasticamente la superficie di attacco e l'impatto di una potenziale esecuzione di bytecode dannoso, contenendo la minaccia.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2025-70314 - CVSS 9.8 (CRITICA)

webfsd 1.21 è vulnerabile a un Buffer Overflow tramite una richiesta appositamente creata. Ciò è dovuto alla variabile filename

Descrizione Originale (EN): webfsd 1.21 is vulnerable to a Buffer Overflow via a crafted request. This is due to the filename variable

Cosa può succedere?

Sfruttando questa vulnerabilità critica, un attaccante potrebbe ottenere il controllo completo del server affetto. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi aziendali essenziali e all'uso del sistema compromesso per ulteriori attacchi alla rete.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.12) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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 servizio webfsd 1.21 in un segmento di rete dedicato, applicando regole firewall stringenti. Limitate l'accesso a questo servizio solo alle sorgenti IP strettamente necessarie e fidate, riducendo drasticamente la superficie di attacco e il potenziale impatto di un'eventuale compromissione.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Termini Alternativi: Classic Buffer Overflow, Unbounded Transfer

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2026-26218 - CVSS 9.8 (CRITICA)

newbee-mall include account amministrativi pre-seeded nello script di inizializzazione del database. Questi account sono provisionati con una password predefinita prevedibile. Le distribuzioni che inizializzano o reimpostano il database utilizzando lo schema fornito e non modificano le credenziali amministrative di default potrebbero consentire a attaccanti non autenticati di accedere come amministratore e ottenere il controllo completo dell'applicazione.

Descrizione Originale (EN): newbee-mall includes pre-seeded administrator accounts in its database initialization script. These accounts are provisioned with a predictable default password. Deployments that initialize or reset the database using the provided schema and fail to change the default administrative credentials may allow unauthenticated attackers to log in as an administrator and gain full administrative control of the application.

Cosa può succedere?

Attaccanti non autenticati potrebbero ottenere il controllo amministrativo completo dell'applicazione, consentendo loro di rubare dati sensibili dei clienti, manipolare le transazioni o interrompere completamente i servizi. Ciò potrebbe causare significative perdite finanziarie e danni irreparabili alla reputazione aziendale.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.07% (Percentile: 0.22) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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 amministrativa di newbee-mall su una rete segmentata o VLAN dedicata. Limitare l'accesso a questo segmento solo agli indirizzi IP autorizzati delle postazioni di lavoro degli amministratori o ai sistemi di gestione interni. Questa misura riduce drasticamente la superficie di attacco, impedendo agli attaccanti non autenticati di raggiungere direttamente l'interfaccia vulnerabile.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2025-70981 - CVSS 9.8 (CRITICA)

CordysCRM 1.4.1 è vulnerabile a SQL Injection nell'interfaccia di query della lista dipendenti (/user/list) tramite il parametro departmentIds.

Descrizione Originale (EN): CordysCRM 1.4.1 is vulnerable to SQL Injection in the employee list query interface (/user/list) via the departmentIds parameter.

Cosa può succedere?

Gli attaccanti potrebbero rubare o manipolare dati sensibili dal database, inclusi informazioni su clienti e dipendenti. In casi gravi, potrebbero ottenere il controllo completo del sistema, causando interruzioni operative significative e gravi danni reputazionali.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.03% (Percentile: 0.08) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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 all'applicazione CordysCRM 1.4.1. Configurare il WAF per ispezionare e bloccare attivamente i tentativi di SQL Injection sul parametro 'departmentIds' nell'interfaccia '/user/list', mitigando l'esposizione finché 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

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

Probabilità di Sfruttamento: high

Termini Alternativi: SQL injection, SQLi

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

CVE-2025-14014 - CVSS 9.8 (CRITICA)

Vulnerabilità di Upload di File Non Limitato con Tipo Pericoloso in NTN Information Processing Services Computer Software Hardware Industry and Trade Ltd. Co. Smart Panel consente l'accesso a funzionalità non correttamente vincolate dalle ACL. Questo problema riguarda Smart Panel: prima del 20251215.

Descrizione Originale (EN): Unrestricted Upload of File with Dangerous Type vulnerability in NTN Information Processing Services Computer Software Hardware Industry and Trade Ltd. Co. Smart Panel allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Smart Panel: before 20251215.

Cosa può succedere?

Un attaccante potrebbe ottenere il controllo completo dei sistemi aziendali interessati. Questo porterebbe al furto di dati sensibili, all'interruzione prolungata dei servizi e alla compromissione totale dell'infrastruttura IT.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.04% (Percentile: 0.13) Disponibili 3 valori storici
Pubblicata:	12/02/2026
Modificata:	13/02/2026
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 del servizio Smart Panel, posizionandolo davanti all'applicazione. Configurare il WAF per ispezionare il traffico in ingresso, bloccando attivamente i tentativi di upload di file con estensioni o contenuti pericolosi e rilevando accessi anomali a funzionalità sensibili non correttamente vincolate. Questo fungerà da controllo compensativo per mitigare la vulnerabilità a livello di rete.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Unrestricted File Upload

Evoluzione EPSS nel Tempo:

Approfondisci su VulnX

4 Vulnerabilità Critiche

5 Top 3 Minacce della Settimana

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

Minaccia #1: CVE-2024-43468 KEV

CVSS: 9.8/10 **EPSS:** 87.5% **Target:** Unknown **Rischio:** 9.5/10

Perché è una minaccia prioritaria:
Questo rappresenta una minaccia critica perché, con un CVSS di 9.8, è attivamente sfruttato (CISA KEV) e presenta un'altissima probabilità di exploit (EPSS 87.5%), rendendolo un rischio immediato e diffuso.

Minaccia #2: CVE-2026-1731 KEV

CVSS: 9.9/10 **EPSS:** 61.4% **Target:** Unknown **Rischio:** 8.8/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché ha un punteggio CVSS quasi massimo (9.9), un'alta probabilità di sfruttamento (EPSS 61.4%) ed è attivamente sfruttata, indicando un rischio immediato e diffuso di compromissione.

Minaccia #3: CVE-2025-40536 KEV

CVSS: 8.1/10 **EPSS:** 71.4% **Target:** Unknown **Rischio:** 8.0/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché, con un CVSS di 8.1 e un'alta probabilità di exploit (71.4%), è già attivamente sfruttata e inclusa nel CISA KEV.

5.1 EPSS Elevato (>95%)

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

5.2 Raccomandazioni

1. **Applicare patch** per tutte le vulnerabilità con **EPSS > 50%**
2. **Monitorare** le CVE aggiunte di recente al catalogo **CISA KEV**
3. Non **Concentrarsi** solamente sulle vulnerabilità di severità **CRITICA** e **ALTA**
4. **Implementare** monitoraggio continuo tramite **VulnX**

5.3 Risorse Aggiuntive

- **Database CVE:** https://vulnx.it/cve/
- **Database KEV:** https://vulnx.it/kev/
- **Catalogo CWE:** https://vulnx.it/cwe/
- **CAPEC:** https://vulnx.it/capec/

VulnX

Piattaforma Avanzata di Cyber Threat Intelligence in lingua italiana

https://vulnx.it

Studio Consi