VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Settimanale

05/10/2026 - 12/10/2026

Generato il: **12/10/2026 20:17**

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.

Sonar

Studio Consi ha sviluppato Sonar, un innovativo **Assets Inventory & Network Scanner agentless**, una soluzione tecnologica avanzata per la gestione e il monitoraggio continuo delle infrastrutture IT.

- Pattugliamento continuo della rete
- Monitoraggio in tempo reale
- Identificazione automatica nuovi asset
- Rilevamento vulnerabilità (CVE/KEV/EPSS)
- Inventario automatizzato
- Modalità agentless (non invasiva)
- Alert proattivi
- Dashboard centralizzata

Registrati gratuitamente

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 12

4 Vulnerabilità Critiche **62**

5 Top 3 Minacce della Settimana **62**
5.1 EPSS Elevato (>95%) 63
5.2 Raccomandazioni 64
5.3 Risorse Aggiuntive 64

1 Sommario Esecutivo

INDICATORE DI RISCHIO SETTIMANALE

ALTO

Riepilogo Settimanale Livello di Minaccia:
Questa settimana sono state identificate 3450 nuove CVE, di cui 358 classificate come critiche (9.0+) e 1222 come alte (7.0-8.9). Il catalogo KEV (Known Exploited Vulnerabilities) è stato aggiornato con 5 nuove voci, e 3 CVE mostrano un'alta probabilità di exploit (EPSS >50%). **Azione Consigliata:** Si raccomanda di prioritizzare la mitigazione immediata delle 5 CVE presenti nel catalogo KEV e delle 3 con EPSS superiore al 50%. Successivamente, affrontare le 358 CVE classificate come critiche per ridurre l'esposizione al rischio.

Metrica	Valore
Totale CVE	**3450**
Critiche	**358**
Alte	**1222**
EPSS >50%	**3**
KEV	**5**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	3,447	–
CVE Modificate	11,210	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	358	11.2%
Alte (7.0-8.9)	1222	38.2%
Medie (4.0-6.9)	1465	45.8%
Basse (0.1-3.9)	155	4.8%
Indicatori di Rischio		
KEV (Exploit Attivi)	5	0.1%
EPSS Elevato (>50%)	3	0.1%

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

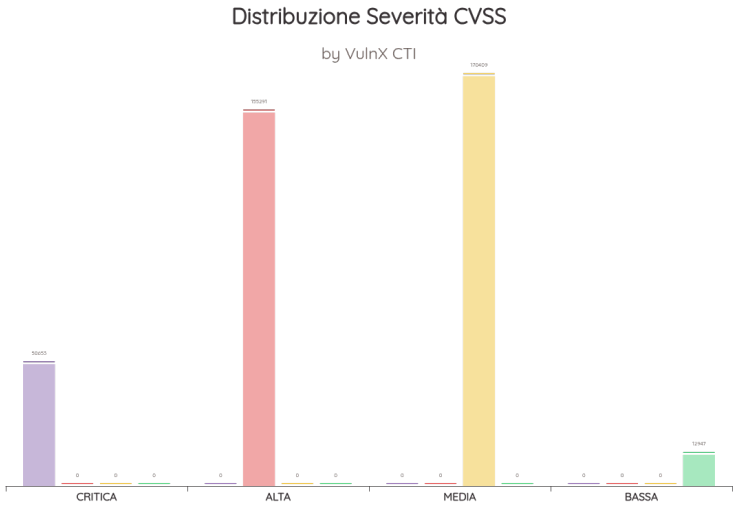
1.2 Panoramica Database (Storico Completo)

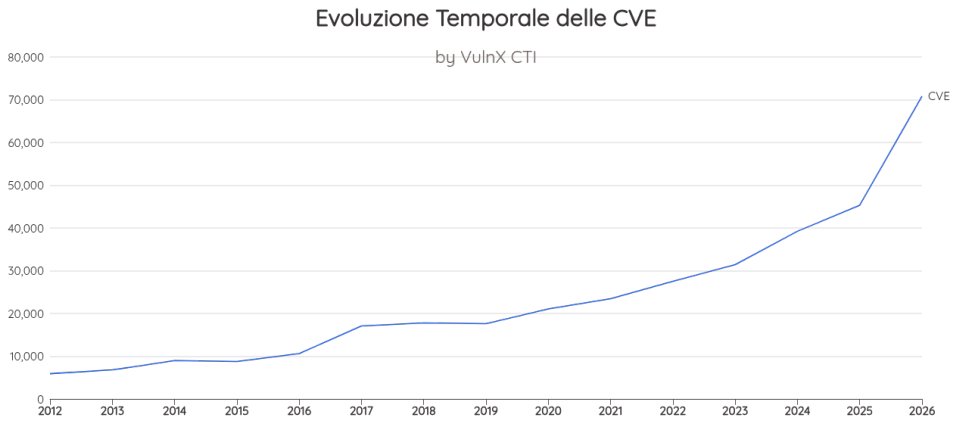
Statistiche complete del database storico su tutte le CVE mai pubblicate:

- **CVE Totali nel Database:** 404,664
- **KEV Totali (Vulnerabilità con Exploit Noti):** 1,741
- **CWE Totali Catalogate:** 969
- **CPE Totali Monitorati:** 2,514,427

Severità	Conteggio	Percentuale
CRITICA	50,653	13.0%
ALTA	155,291	39.9%
MEDIA	170,409	43.8%
BASSA	12,947	3.3%

Tabella 1: *Distribuzione per Severità*


Distribuzione Severità CVSS
by VulnX CTI
CRITICA
ALTA
MEDIA
BASSA


Evoluzione Temporale delle CVE
by VulnX CTI
80,000
70,000
60,000
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:

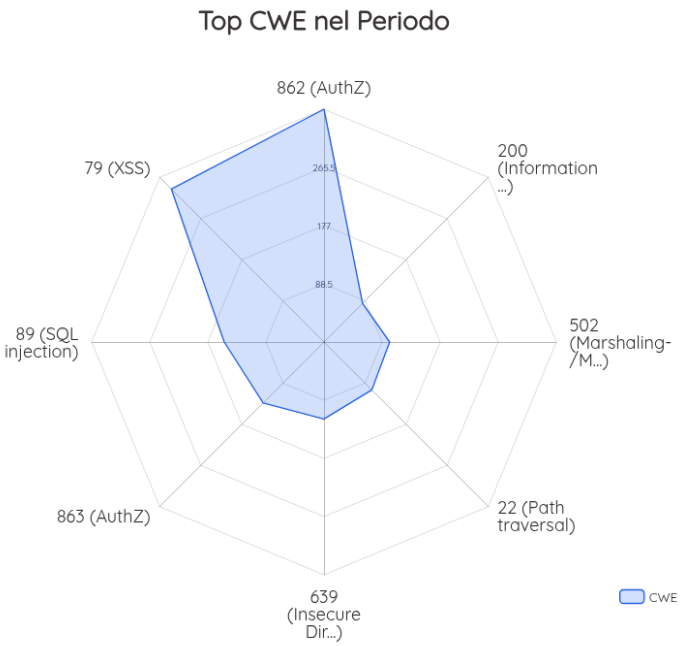


Figura 1: *Distribuzione Top CWE - Grafico Radar*

3.2 Analisi Approfondita delle Debolezze (CWE)

Le debolezze più comuni con raccomandazioni di difesa.

20

Improper Input Validation

▶ **Occorrenze:** 45

Raccomandazioni di Difesa

- Ecco 2-3 raccomandazioni specifiche e attuabili per CWE-20 - Improper Input Validation:
- N/A**Implementare una validazione rigorosa dell'input lato server:**Validare e sanificare tutti i dati forniti dall'utente (e da altre fonti esterne) utilizzando liste bianche (whitelist) per tipi di dati, formati e lunghezze attesi, rifiutando qualsiasi input non conforme.
- N/A**Configurare un Web Application Firewall (WAF):**Distribuire e ottimizzare le regole di un WAF per rilevare e bloccare tentativi di attacco comuni basati su input malevolo, come SQL Injection, Cross-Site Scripting (XSS) e Path Traversal.
- N/A**Integrare SAST e DAST nella pipeline CI/CD:**Utilizzare strumenti di Static Application Security Testing (SAST) e Dynamic Application Security Testing (DAST) per identificare automaticamente la mancanza o l'errata implementazione della validazione dell'input durante lo sviluppo e il testing.

532

Insertion of Sensitive Information into Log File

- **Occorrenze:** 17

Raccomandazioni di Difesa

- Ecco 3 raccomandazioni specifiche e attuabili per la debolezza CWE-532:
- N/A**Pratiche di Sviluppo:**Implementare la mascheratura o la redazione automatica dei dati sensibili (es. credenziali, PII, numeri di carte di credito) a livello di codice, *prima* della loro registrazione nei log.
- N/A**Policy e Controlli:**Adottare una policy di logging restrittiva che specifichi chiaramente quali informazioni possono essere loggate e condurre revisioni del codice mirate per prevenire la registrazione accidentale di dati sensibili.
- N/A**Configurazione Strumenti:**Configurare i framework di logging (es. Log4j, Serilog) per escludere o offuscare automaticamente i campi contenenti dati sensibili e limitare l'uso di livelli di log dettagliati (es. DEBUG, TRACE) negli ambienti di produzione.

732

Incorrect Permission Assignment for Critical Resource

▶ **Occorrenze:** 13

Raccomandazioni di Difesa

▶ Ecco 3 raccomandazioni specifiche e attuabili per CWE-732:

▶ N/A**Implementare il principio del minimo privilegio (Least Privilege)**per tutti gli utenti, processi e servizi, garantendo che abbiano solo le autorizzazioni strettamente necessarie per svolgere le proprie funzioni.

▶ N/A**Adottare un modello di controllo degli accessi basato sui ruoli (RBAC - Role-Based Access Control)**per gestire le autorizzazioni in modo centralizzato e coerente, assegnando permessi a ruoli anziché direttamente agli utenti.

▶ N/A**Definire e applicare configurazioni di sicurezza standard (baseline)**per le autorizzazioni delle risorse critiche e condurre audit regolari per verificarne la conformità e identificare eventuali deviazioni.

319

Cleartext Transmission of Sensitive Information

▶ **Occorrenze:** 12

Raccomandazioni di Difesa

▶ Ecco 3 raccomandazioni specifiche e attuabili per CWE-319:

▶ N/A**Imporre l'uso di HTTPS/TLS per tutte le comunicazioni web e API**, configurando i server (es. Apache, Nginx, IIS) per reindirizzare automaticamente il traffico HTTP e utilizzare certificati TLS validi.

▶ N/A**Crittografare tutte le comunicazioni interne tra servizi e con i database**utilizzando TLS/SSL, anche all'interno di reti private, per proteggere i dati sensibili in transito.

▶ N/A**Disabilitare i protocolli di comunicazione non sicuri**(es. HTTP, FTP, Telnet) sui server e bloccare le relative porte a livello di firewall, ove non strettamente necessari e non sostituibili con alternative crittografate.

611

Improper Restriction of XML External Entity Reference

▶ **Occorrenze:** 6

Raccomandazioni di Difesa

▶ Ecco 2 raccomandazioni specifiche e attuabili per CWE-611:

▶ N/A**Disabilitare le entità esterne nei parser XML**: Configurare i parser XML utilizzati nell'applicazione per disabilitare completamente la risoluzione delle entità esterne (DTD, XEE) o limitarla rigorosamente a risorse locali e fidate. Questa è la misura più efficace e diretta per prevenire gli attacchi XXE.

▶ N/A**Validazione rigorosa dell'input XML tramite schema**: Implementare la validazione dell'input XML rispetto a uno schema (XSD) predefinito e rigoroso. Assicurarsi che lo schema non consenta la definizione o l'uso di entità esterne non autorizzate e che l'input aderisca strettamente alla struttura attesa.

297

Improper Validation of Certificate with Host Mismatch

▶ **Occorrenze:** 4

Raccomandazioni di Difesa

▶ Ecco 3 raccomandazioni specifiche e pratiche per CWE-297:

▶ N/A**Sviluppo:**Implementare la validazione rigorosa del nome host (hostname validation) in tutte le connessioni TLS/SSL effettuate dalle applicazioni, assicurandosi che il nome host del certificato corrisponda all'endpoint previsto.

▶ N/A**Configurazione/Strumenti:**Utilizzare librerie e framework TLS/SSL aggiornati che applicano la validazione del nome host per impostazione predefinita e non disabilitare mai esplicitamente tali controlli di sicurezza.

▶ N/A**Processi:**Integrare test specifici per la corretta validazione del nome host nelle pipeline CI/CD e nelle revisioni del codice, per prevenire regressioni o configurazioni errate.

3.3 CVE del Periodo Analizzato

Trovate **3447** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **25** CVE:

CVE-2026-109321 - CVSS 9.1 (CRITICA)

Il plugin Grav Login OAuth (grav-plugin-login-oauth) prima della versione 1.4.3 configura gli account OAuth come utenti Grav ordinari con un nome utente deterministico <provider>.<id> e un hash MD5 senza sale dell'identificatore del provider come password, senza disabilitare l'accesso tramite password. Gli attaccanti remoti non autenticati che apprendono o indovinano un identificatore del provider possono riprodurre queste credenziali e accedere, ottenendo il controllo amministrativo sugli account privilegiati.

Descrizione Originale (EN): Grav Login OAuth plugin (grav-plugin-login-oauth) before 1.4.3 provisions OAuth accounts as ordinary Grav users with a deterministic <provider>.<id> username and an unsalted MD5 hash of the provider identifier as the password, without disabling password login. Unauthenticated remote attackers who learn or guess a provider identifier can reproduce these credentials and log in, gaining administrative control of privileged accounts.

Cosa può succedere?
Gli attaccanti remoti potrebbero ottenere il controllo amministrativo completo del sistema Grav. Questo permetterebbe loro di accedere a dati sensibili, alterare contenuti, o causare interruzioni significative del servizio e gravi danni alla reputazione aziendale.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
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, implementate un Web Application Firewall (WAF) o un reverse proxy con autenticazione aggiuntiva (es. multi-fattore) davanti all'istanza Grav. Questo permetterà di ispezionare e bloccare tentativi di accesso non autorizzati o sospetti prima che raggiungano l'applicazione vulnerabile, fornendo un livello di controllo degli accessi preventivo e robusto.

CVSS Metrics

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

CWE - Common Weakness Enumeration

1391: **Use of Weak Credentials**

Approfondisci su VulnX

CVE-2026-109318 - CVSS 8.8 (ALTA)

Grav Git Sync 1.0.2 fino alla 3.4.12 contiene una vulnerabilità di command injection che consente agli editor di contenuti autenticati di eseguire comandi OS inserendo sostituzioni shell nei campi del profilo. Quando è abilitata la modalità gravuser o gravfull, gli attaccanti possono impostare un nome utente, nome completo o email dannosi che raggiungono PHP exec() tramite git commit –author, eseguendo comandi come l'account del server web.

Descrizione Originale (EN): Grav Git Sync 1.0.2 through 3.4.12 contains a command injection vulnerability that allows authenticated content editors to execute OS commands by injecting shell substitutions into profile fields. When the gravuser or gravfull author mode is enabled, attackers can set a malicious username, full name, or email that reaches PHP exec() via git commit –author, running commands as the web-server account.

Cosa può succedere?

Un attaccante autenticato potrebbe ottenere il controllo completo del server web, consentendo il furto di dati sensibili, la manipolazione dei contenuti del sito o la disabilitazione dei servizi. Ciò potrebbe portare a gravi interruzioni operative e all'utilizzo del server compromesso per lanciare ulteriori attacchi interni.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolare il server che ospita l'applicazione Grav Git Sync in un segmento di rete dedicato e strettamente controllato, come una DMZ o una VLAN isolata. Questo limiterà drasticamente la capacità di un attaccante di accedere ad altre risorse interne critiche o di esfiltrare dati, anche in caso di successo dell'iniezione di comandi.

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

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

Approfondisci su VulnX

CVE-2026-109305 - CVSS 8.8 (ALTA)

Craft CMS dalla versione 5.10.2 fino alla 5.10.14 contiene un bypass del sandbox di Twig che consente agli utenti non amministratori di invocare callable PHP tramite gli operatori ”has some” e ”has every”. Gli utenti con il permesso System Messages possono fornire callable a due argomenti come passthru o system in template sandboxati per eseguire codice come l’utente web.

Descrizione Originale (EN): Craft CMS from 5.10.2 before 5.10.14 contains a Twig sandbox bypass that allows non-admin users to invoke PHP callables through the ’has some’ and ’has every’ operators. Users with the System Messages permission can supply two-argument callables such as passthru or system in sandboxed templates to execute code as the web user.

Cosa può succedere?

Un utente non amministratore con permessi specifici potrebbe eseguire codice arbitrario sul server, ottenendo il controllo completo del sito web. Ciò consentirebbe il furto di dati sensibili, la compromissione del sistema e potenziali interruzioni dei servizi, con gravi danni alla reputazione aziendale.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare rigorosi controlli di accesso a livello di rete per l’interfaccia amministrativa di Craft CMS. Limitare l’accesso a tale interfaccia solo a indirizzi IP interni fidati o tramite una Virtual Private Network (VPN) per ridurre significativamente l’esposizione a potenziali aggressori esterni. Questo ostacola la capacità di utenti non autorizzati di raggiungere e sfruttare la vulnerabilità.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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-2026-109308 - CVSS 8.8 (ALTA)

Craft CMS 4.0.0 prima della 4.18.7 e 5.0.0 prima della 5.10.14 invia il parametro di richiesta raw 'updates' in AppController::actionCacheUpdates a UpdatesModel senza l'uso di Component::cleanseConfig(), consentendo l'iniezione di comportamenti e gestori di eventi. Gli utenti autenticati del control panel con il permesso performUpdates o accesso all'utility Updates possono fornire le chiavi 'as' o 'on', come un gadget AttributeTypecastBehavior, per eseguire codice arbitrario.

Descrizione Originale (EN): Craft CMS 4.0.0 before 4.18.7 and 5.0.0 before 5.10.14 passes the raw 'updates' request parameter in AppController::actionCacheUpdates to UpdatesModel without Component::cleanseConfig(), allowing behavior and event-handler injection. Authenticated control panel users with the performUpdates permission or Updates-utility access can supply 'as' or 'on' keys, such as an AttributeTypecastBehavior gadget, to execute arbitrary code.

Cosa può succedere?
Un utente malintenzionato autenticato potrebbe eseguire codice arbitrario sul server, ottenendo il controllo completo del sistema. Ciò potrebbe portare al furto di dati sensibili, alla compromissione del sito web o alla sua interruzione, causando gravi danni reputazionali e finanziari all'azienda.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Rafforzare i controlli di accesso per il pannello di controllo di Craft CMS. Limitare rigorosamente l'assegnazione del permesso 'performUpdates' e l'accesso all'utility 'Updates' solo agli account amministrativi strettamente necessari, e implementare l'autenticazione a più fattori (MFA) per tutti gli utenti privilegiati.

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

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

Approfondisci su VulnX

CVE-2026-109372 - CVSS 8.7 (ALTA)

ZITADEL 4.x prima della versione 4.19.2 e 3.x fino alla 3.4.15 contiene un bypass dell'autenticazione nell'intent di callback dell'identità SAML-provider, che verifica la firma dell'asserzione utilizzando il provider indicato nell'URL della richiesta ma risolve l'utente dall'intent di login senza verificare che corrispondano. Gli attaccanti con permesso di organizzazione-amministratore possono registrare un provider SAML con la propria chiave di firma per ottenere sessioni autenticati come qualsiasi utente collegato a un altro provider SAML sull'istanza, inclusi in altre organizzazioni.

Descrizione Originale (EN): ZITADEL 4.x before 4.19.2 and 3.x through 3.4.15 contains an authentication bypass in the SAML identity-provider intent callback, which verifies the assertion signature using the provider named in the request URL but resolves the user from the login intent without checking they match. Attackers with organization-administrator permission can register a SAML provider with their own signing key to obtain authenticated sessions as any user linked to another SAML provider on the instance, including in other organizations.

Cosa può succedere?
Un attaccante con permesso di amministratore di organizzazione può impersonare qualsiasi utente del sistema, inclusi quelli con ruoli critici. Questo permette l'accesso non autorizzato a dati sensibili, la manipolazione di informazioni o la compromissione di sistemi e servizi aziendali, con gravi conseguenze per la sicurezza e la reputazione.

Punteggio CVSS:	8.7 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare un monitoraggio e una registrazione robusti per i processi di autenticazione di ZITADEL, concentrandosi in particolare sugli intenti di callback dell'identità SAML. Configurare avvisi per rilevare qualsiasi discrepanza tra il provider SAML indicato nell'URL della richiesta e l'utente risolto dall'intento di login, o per pattern di accesso insoliti. Questo aiuterà a identificare e rispondere rapidamente a tentativi di bypass dell'autenticazione.

CVSS Metrics

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

CWE - Common Weakness Enumeration

287: **Improper Authentication**

Probabilità di Sfruttamento: high

Termini Alternativi: authentification, AuthN, AuthC

Approfondisci su VulnX

CVE-2026-109371 - CVSS 8.2 (ALTA)

ZITADEL 3.0.0 prima della versione 4.18.0 contiene una vulnerabilità di autenticazione mancante nel hosted Login V1 UI, dove il gestore change-username agisce sull'account associato a un flusso di login prima che venga verificato qualsiasi fattore. Gli attaccanti non autenticati possono inviare il nome utente di una vittima e successivamente postare un nuovo username per rinominare qualsiasi utente umano attivo, inclusi gli amministratori, bloccandoli dall'accesso.

Descrizione Originale (EN): ZITADEL 3.0.0 before 4.18.0 contains a missing authentication vulnerability in the hosted Login V1 UI, where the change-username handler acts on the account bound to a login flow before any factor is verified. Unauthenticated attackers can submit a victim's login name and then post a new username to rename any active human user, including administrators, locking them out.

Cosa può succedere?

Un attaccante non autenticato può rinominare gli account di qualsiasi utente attivo, inclusi gli amministratori, impedendo loro l'accesso. Questo causa una grave interruzione dei servizi e delle operazioni aziendali, poiché il personale legittimo viene bloccato dal sistema.

Punteggio CVSS:	8.2 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) o un API Gateway davanti all'istanza ZITADEL. Configurare queste soluzioni per intercettare e bloccare le richieste dirette all'endpoint di cambio username che non provengono da sessioni autenticate o che mostrano comportamenti anomali. Questo fungerà da controllo compensativo, aggiungendo un livello di protezione esterno contro tentativi di rinominare account senza autenticazione valida.

CVSS Metrics

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

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-109313 - CVSS 8.1 (ALTA)

Il plugin Grav Login 2.7.0 fino alla versione 3.9.9 presenta una vulnerabilità di bypass dell'autenticazione che consente agli attaccanti con una password valida di saltare l'autenticazione a due fattori tramite il ripristino del cookie remember-me. Gli attaccanti possono ottenere un cookie remember-me persistente dopo il passaggio della password e ripristinarlo come sessione completamente autorizzata senza completare il secondo fattore.

Descrizione Originale (EN): Grav Login plugin 2.7.0 before 3.9.9 contains an authentication bypass vulnerability that allows attackers with a valid password to skip two-factor authentication through remember-me cookie restoration. Attackers can obtain a persistent remember-me cookie after the password step and restore it as a fully authorized session without completing the second factor.

Cosa può succedere?

Un aggressore in possesso di una password valida può aggirare l'autenticazione a due fattori, ottenendo accesso completo e persistente ai sistemi come un utente autorizzato. Ciò può portare al furto di dati sensibili, alla compromissione di account privilegiati e all'accesso non autorizzato a funzionalità o informazioni riservate.

Punteggio CVSS:	8.1 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
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 non è disponibile una patch, implementate un controllo degli accessi a livello di rete o applicazione (es. tramite un WAF o un reverse proxy) che imponga un'autenticazione a più fattori esterna *prima* di raggiungere l'istanza di Grav. Questo aggiunge un ulteriore strato di sicurezza, assicurando che anche in caso di bypass del 2FA interno del plugin, l'accesso non autorizzato sia impedito da un meccanismo di autenticazione separato.

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:** none

CWE - Common Weakness Enumeration

287: **Improper Authentication**

Probabilità di Sfruttamento: high

Termini Alternativi: authentification, AuthN, AuthC

Approfondisci su VulnX

CVE-2026-109357 - CVSS 8.1 (ALTA)

LibreNMS prima della versione 26.9.0 contiene un'iniezione di filtro LDAP in modalità ldap-authorization e ad-authorization perché i nomi utente vengono inseriti non escapati nei filtri di ricerca LDAP e l'autenticazione verifica solo l'esistenza dell'utente. Quando REMOTE_USER non viene inoltrato, gli attaccanti non autenticati possono inviare un nome utente con caratteri jolly tramite HTTP Basic Authorization (PHP_AUTH_USER) per corrispondere a tutti gli utenti e gruppi e ottenere accesso amministrativo.

Descrizione Originale (EN): LibreNMS before 26.9.0 contains an LDAP filter injection in ldap-authorization and ad-authorization modes because usernames are inserted unescaped into LDAP search filters and authentication only checks user existence. When REMOTE_USER is not forwarded, unauthenticated attackers can send a wildcard username via HTTP Basic Authorization (PHP_AUTH_USER) to match all users and groups and gain admin access.

Cosa può succedere?

Un attaccante non autenticato potrebbe ottenere pieno accesso amministrativo al sistema LibreNMS. Ciò permetterebbe il furto di dati sensibili di monitoraggio, la manipolazione delle configurazioni di rete e la potenziale compromissione di altri sistemi aziendali, causando interruzioni del servizio e gravi danni alla reputazione.

Punteggio CVSS:	8.1 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare un Web Application Firewall (WAF) a protezione dell'istanza di LibreNMS. Configurare il WAF per ispezionare e filtrare attivamente i nomi utente nelle richieste di autenticazione HTTP Basic, bloccando qualsiasi tentativo che includa caratteri jolly o pattern di iniezione LDAP. Questo agisce come controllo compensativo, prevenendo lo sfruttamento della vulnerabilità da parte di attaccanti non autenticati.

CVSS Metrics

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

CWE - Common Weakness Enumeration

90: **Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')**

Approfondisci su VulnX

CVE-2026-109346 - CVSS 8.1 (ALTA)

better-auth dalla versione 1.3.8-beta.3 prima della 1.7.0-rc.3 contiene una vulnerabilità di rappresentazione errata dell'interfaccia utente nel plugin deviceAuthorization perché GET /device omette il client_id e lo scope della richiesta. Gli attaccanti possono avviare una richiesta di dispositivo tramite /device/code, ingannare gli utenti autenticati ad approvare il codice, quindi riscattarlo su /device/token per ottenere un token di sessione attiva.

Descrizione Originale (EN): better-auth from 1.3.8-beta.3 before 1.7.0-rc.3 contains a UI misrepresentation vulnerability in the deviceAuthorization plugin because GET /device omits the requesting client_id and scope. Attackers can start a device request via /device/code, trick signed-in users into approving the code, then redeem it at /device/token for a live session token.

Cosa può succedere?

Un aggressore potrebbe impersonare un utente autenticato, ottenendo accesso non autorizzato a dati e risorse aziendali riservate. Ciò può portare al furto di informazioni sensibili, frodi o alla compromissione di sistemi critici.

Punteggio CVSS:	8.1 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
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 una segmentazione di rete rigorosa per gli endpoint di autorizzazione del dispositivo (‘/device‘, ‘/device/code‘) del servizio ‘better-auth‘. Assicurarsi che questi endpoint siano accessibili solo da reti interne fidate o da indirizzi IP specifici e autorizzati. Questo ridurrà drasticamente la superficie di attacco, impedendo agli attacc

CVSS Metrics

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

CWE - Common Weakness Enumeration

451: **User Interface (UI) Misrepresentation of Critical Information**

Approfondisci su VulnX

CVE-2026-109334 - CVSS 8.1 (ALTA)

SurrealDB prima della versione 3.3.0 non verifica lo namespace o il database selezionato dal chiamante rispetto al livello con cui un utente di sistema a livello di namespace o database si è autenticato, consentendo l'accesso cross-tenant. Un attaccante autenticato può impostare gli header Surreal-NS/Surreal-DB su /sql o chiamare il metodo RPC use per leggere, creare, modificare e eliminare righe e leggere i valori DEFINE PARAM in un altro tenant dove i PERMISSIONS delle tabelle lo consentono.

Descrizione Originale (EN): SurrealDB before 3.3.0 does not check the caller-selected namespace or database against the level at which a namespace- or database-level system user authenticated, allowing cross-tenant access. An authenticated attacker can set the Surreal-NS/Surreal-DB headers on /sql or call the RPC use method to read, create, modify, and delete rows and read DEFINE PARAM values in another tenant where table PERMISSIONS allow it.

Cosa può succedere?

Un attaccante autenticato può accedere e manipolare i dati di altri clienti o dipartimenti all'interno della stessa piattaforma. Ciò comporta il rischio di furto di dati sensibili, violazioni della privacy e interruzioni dei servizi, con gravi conseguenze legali e reputazionali per l'azienda.

Punteggio CVSS:	8.1 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
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 accesso cross-tenant, isolare le istanze di SurrealDB in segmenti di rete distinti per ciascun tenant o applicazione critica. Implementare regole firewall stringenti per consentire l'accesso al database solo da indirizzi IP e servizi specifici e autorizzati. Ciò limita drasticamente la superficie di attacco e previene la navigazione non autorizzata tra i namespace.

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:** none

CWE - Common Weakness Enumeration

639: **Authorization Bypass Through User-Controlled Key**

Probabilità di Sfruttamento: high

Termini Alternativi: Insecure Direct Object Reference / IDOR, Broken Object Level Authorization / BOLA, Horizontal Authorization

Approfondisci su VulnX

CVE-2026-109343 - CVSS 8.1 (ALTA)

SurrealDB prima della versione 3.3.0 consente l'accesso cross-tenant perché l'istruzione SurrealQL USE cambia il contesto di una sessione a qualsiasi namespace/database senza verificare che il livello di autenticazione del chiamante lo copra. Gli utenti autenticati di namespace, database o record possono passare a un altro tenant e leggere, creare, aggiornare o eliminare righe nelle tabelle i cui PERMISSIONS consentono, come PERMISSIONS FULL.

Descrizione Originale (EN): SurrealDB before 3.3.0 allows cross-tenant access because the SurrealQL USE statement switches a session to any namespace/database without checking that the caller's authenticated level covers it. Authenticated namespace, database, or record users can switch to another tenant and read, create, update, or delete rows in tables whose PERMISSIONS allow it, such as PERMISSIONS FULL.

Cosa può succedere?

Un utente autenticato potrebbe accedere ai dati di altri clienti o dipartimenti all'interno del sistema. Ciò permetterebbe di leggere, modificare o persino eliminare informazioni sensibili appartenenti ad altri tenant, causando gravi violazioni della privacy, furto di dati e potenziali interruzioni operative.

Punteggio CVSS:	8.1 (ALTA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Raccomandazione di Sicurezza: Implementate controlli di accesso di rete rigorosi (es. regole firewall, security groups) per limitare l'accesso all'istanza di SurrealDB unicamente alle applicazioni e ai servizi autorizzati, provenienti da indirizzi IP fidati. Questo riduce drasticamente la superficie di attacco, mitigando il rischio di accesso cross-tenant anche da parte di utenti autenticati, agendo come controllo compensativo a livello infrastrutturale.

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:** none

CWE - Common Weakness Enumeration

639: **Authorization Bypass Through User-Controlled Key**

Probabilità di Sfruttamento: high

Termini Alternativi: Insecure Direct Object Reference / IDOR, Broken Object Level Authorization / BOLA, Horizontal Authorization

Approfondisci su VulnX

CVE-2026-108907 - CVSS 10.0 (CRITICA)

È stata individuata una vulnerabilità in Netcore NR268 1.7.121109. Interessata è la funzione user_ok del componente CGI Execution. Questa manipolazione provoca un'autenticazione impropria. L'attacco può essere avviato da remoto. L'exploit è stato divulgato pubblicamente 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 determined in Netcore NR268 1.7.121109. Affected is the function user_ok of the component CGI Execution. This manipulation causes improper authentication. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?

Lo sfruttamento di questa vulnerabilità consente a un attaccante remoto di bypassare l'autenticazione e ottenere il controllo completo dei dispositivi Netcore vulnerabili. Ciò può portare al furto di dati sensibili, all'interruzione dei servizi di rete critici e alla compromissione dell'intera rete aziendale.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Isolate immediatamente il dispositivo Netcore NR268 in una rete segmentata (es. VLAN dedicata) e configurate regole firewall stringenti. Permettete l'accesso al dispositivo solo da indirizzi IP o sottoreti di gestione strettamente autorizzati e interni, bloccando qualsiasi accesso non necessario da internet o da altre reti non fidate. Questo ridurrà drasticamente la superficie di attacco e limiterà la possibilità di sfruttamento remoto dell'autenticazione impropria.

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

287: **Improper Authentication**

Probabilità di Sfruttamento: high

Termini Alternativi: authentification, AuthN, AuthC

Approfondisci su VulnX

CVE-2026-108892 - CVSS 10.0 (CRITICA)

È stata individuata una vulnerabilità in Linksys E1700 1.0.0.4.003. Questa vulnerabilità riguarda la funzione ssid1MACFilter del file /goform/ssid1MACFilter del componente Mac Filter. La manipolazione dell'argomento newap_text_%d provoca un overflow del buffer basato su stack. L'attacco può essere avviato da remoto. L'exploit è stato divulgato pubblicamente 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 determined in Linksys E1700 1.0.0.4.003. This vulnerability affects the function ssid1MACFilter of the file /goform/ssid1MACFilter of the component Mac Filter. This manipulation of the argument newap_text_%d causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?
Un attaccante remoto potrebbe ottenere il controllo completo dei router Linksys vulnerabili, compromettendo l'intera rete aziendale. Ciò potrebbe portare a gravi furti di dati, interruzioni dei servizi critici e l'uso dei dispositivi come base per ulteriori attacchi interni.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Data la gravità della vulnerabilità e l'assenza di una patch, si raccomanda di isolare il router Linksys E1700 in un segmento di rete dedicato e altamente ristretto, come una DMZ separata. Implementare regole firewall stringenti per limitare al minimo indispensabile il traffico da e verso il dispositivo, impedendo in particolare che possa avviare connessioni verso reti interne sensibili.

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

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

Probabilità di Sfruttamento: high

Termini Alternativi: Buffer Overflow, buffer overrun, memory safety

---

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-108804 - CVSS 10.0 (CRITICA)

È stata rilevata una vulnerabilità in TRENDnet TEW-751DR, TEW-752DRU e TEW733GR 1.03B01/1.03B03. È interessata la funzione fwrite del file pigwidgeon.cgi del componente Web Management Backend. La manipolazione dell'argomento service può portare a un'iniezione di comandi OS. È possibile lanciare l'attacco da remoto. Lo sfruttamento è ora pubblico e può essere utilizzato. Il fornitore conferma: "Poiché questo router è stato messo in End of Life (EOL) nel 2011, non abbiamo modo di verificare se tale vulnerabilità esiste. Notificheremo i nostri clienti di una potenziale vulnerabilità su questo prodotto." Questa vulnerabilità riguarda esclusivamente prodotti che non sono più supportati dal manutentore.

Descrizione Originale (EN): A vulnerability was detected in TRENDnet TEW-751DR, TEW-752DRU and TEW733GR 1.03B01/1.03B03. Affected is the function fwrite of the file pigwidgeon.cgi of the component Web Management Backend. The manipulation of the argument service results in os command injection. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor confirms: 'As this router was EOL'd in 2011, we have no way of testing if such vulnerability exists. We will notify our customers of a potential vulnerability on this product.' This vulnerability only affects products that are no longer supported by the maintainer.

Cosa può succedere?

Un attaccante remoto può ottenere il controllo completo del router, compromettendo l'intera rete aziendale. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi di rete critici o all'utilizzo del dispositivo come punto di partenza per ulteriori attacchi interni.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	2.39% (Percentile: 0.83)
Pubblicata:	12/10/2026
Modificata:	12/10/2026
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 TRENDnet vulnerabili su una rete di gestione separata e non accessibile da Internet. Implementare regole firewall stringenti per consentire l'accesso all'interfaccia di gestione solo da indirizzi IP specifici e fidati all'interno della rete interna, riducendo drasticamente la superficie di attacco.

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Termini Alternativi: Command injection

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

Probabilità di Sfruttamento: high

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

Approfondisci su VulnX

CVE-2026-85955 - CVSS 9.9 (CRITICA)

Progress MarkLogic Server 12.x rilasci prima di 12.1.0 e le versioni 11.x prima di 11.3.7 consentono a un attaccante remoto con accesso all'esecuzione di query di invocare una funzione di valutazione XQuery senza il privilegio di valutazione aggiuntivo richiesto, il che potrebbe portare all'esecuzione di codice lato server con privilegi elevati.

Descrizione Originale (EN): Progress MarkLogic Server 12.x releases before 12.1.0 and 11.x releases before 11.3.7 allow a remote attacker with query-execution access to invoke an XQuery evaluation function without the additional required evaluation privilege, which could result in server-side code execution with elevated permissions.

Cosa può succedere?

Un attaccante remoto può ottenere il controllo completo del server MarkLogic, consentendo il furto, la manipolazione o la cancellazione di dati sensibili. Ciò può portare a interruzioni dei servizi critici e alla compromissione dell'integrità dell'intero sistema aziendale.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
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 server MarkLogic vulnerabili in una rete segmentata o DMZ, limitando rigorosamente l'accesso in ingresso per l'esecuzione di query solo alle sorgenti IP strettamente necessarie e autorizzate. Questo ridurrà significativamente la superficie di attacco e la probabilità che un attaccante remoto possa raggiungere il server per sfruttare la vulnerabilità.

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

269: **Improper Privilege Management**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-85948 - CVSS 9.9 (CRITICA)

Progress MarkLogic Server 12.x rilasci prima di 12.1.0 e le versioni 11.x prima di 11.3.7 presentano una vulnerabilità di iniezione XQuery in un percorso del package API di Management deprecato. Un attaccante remoto con privilegi manage-user-level potrebbe sfruttare questa falla per ottenere un controllo amministrativo non autorizzato persistente.

Descrizione Originale (EN): Progress MarkLogic Server 12.x releases before 12.1.0 and 11.x releases before 11.3.7 contain an XQuery injection flaw in a deprecated Management API package path. A remote attacker with manage-user-level privileges could exploit this flaw to obtain persistent unauthorized administrative control.

Cosa può succedere?

Un attaccante remoto potrebbe ottenere il controllo amministrativo completo del server MarkLogic, consentendo il furto, la modifica o la cancellazione di dati sensibili. Ciò potrebbe causare gravi interruzioni dei servizi aziendali, perdita di dati critici e un persistente accesso non autorizzato al sistema.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare una rigorosa segmentazione di rete per isolare le interfacce di gestione del server MarkLogic, in particolare i percorsi API deprecati, dall'accesso generale della rete. Limitare le connessioni in ingresso a queste interfacce esclusivamente a un set ristretto di host amministrativi fidati o a reti di gestione dedicate. Ciò riduce significativamente la superficie di attacco per lo sfruttamento remoto, anche in presenza di privilegi utente esistenti.

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

269: **Improper Privilege Management**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-85947 - CVSS 9.9 (CRITICA)

Progress MarkLogic Server 12.x rilasci prima della 12.1.0 e le versioni 11.x prima della 11.3.7 contengono una vulnerabilità di autorizzazione in alcune operazioni di gestione dei forest. Un attaccante remoto con privilegi di gestione dei forest potrebbe sfruttare questa vulnerabilità per creare un account amministratore non autorizzato persistente, con il potenziale di ottenere un controllo amministrativo completo e non autorizzato sul server.

Descrizione Originale (EN): Progress MarkLogic Server 12.x releases before 12.1.0 and 11.x releases before 11.3.7 contain an authorization flaw in certain forest-management operations. A remote attacker with forest-management privileges could exploit this flaw to create a persistent unauthorized administrator account, potentially resulting in complete unauthorized administrative control of the server.

Cosa può succedere?

Un attaccante con privilegi specifici potrebbe creare un account amministratore segreto e persistente, ottenendo il controllo completo e non autorizzato del server MarkLogic. Questo permetterebbe il furto o la manipolazione di dati sensibili, l'interruzione dei servizi critici e l'uso del server come punto di accesso per ulteriori attacchi all'intera rete aziendale.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare una rigorosa segmentazione della rete per il server Progress MarkLogic, isolandolo in una zona di sicurezza dedicata. Limitare l'accesso alle interfacce di gestione del server esclusivamente a host e utenti strettamente autorizzati tramite firewall e liste di controllo accessi (ACL), riducendo significativamente la superficie di attacco e la possibilità per un attaccante remoto di sfruttare questa vulnerabilità.

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

269: **Improper Privilege Management**

Probabilità di Sfruttamento: medium

Approfondisci su VulnX

CVE-2026-108914 - CVSS 9.9 (CRITICA)

È stata scoperta una vulnerabilità in Edimax BR-6208AC 1.32. A rischio è una funzionalità sconosciuta del file /goform/formWISiteSurvey. La manipolazione dell'argomento ifname provoca un overflow del buffer. È possibile sfruttare questa vulnerabilità da remoto. L'exploit è stato pubblicato e può essere utilizzato. Il fornitore è stato contattato tempestivamente riguardo a questa divulgazione, ma non ha risposto in alcun modo. Questa vulnerabilità riguarda esclusivamente prodotti che non sono più supportati dal manutentore.

Descrizione Originale (EN): A flaw has been found in Edimax BR-6208AC 1.32. Affected by this issue is some unknown functionality of the file /goform/formWISiteSurvey. This manipulation of the argument ifname causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.

Cosa può succedere?

Un attaccante remoto potrebbe ottenere il controllo completo del router, compromettendo l'intera rete aziendale. Ciò consentirebbe il furto di dati sensibili, l'interruzione dei servizi critici e l'accesso non autorizzato ai sistemi interni, con gravi conseguenze operative e reputazionali.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
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 natura critica della vulnerabilità e la disponibilità di un exploit remoto, si raccomanda di isolare immediatamente il dispositivo Edimax BR-6208AC in un segmento di rete dedicato. Implementate rigorose regole di firewall per limitare l'accesso al dispositivo solo alle sorgenti di traffico strettamente necessarie e fidate, bloccando ogni accesso non essenziale, in particolare dall'esterno.

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

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-2026-108896 - CVSS 9.9 (CRITICA)

È stata individuata una vulnerabilità in Linksys E1700 1.0.0.4.003. Questa interessa la funzione setLinksysIpv6 del file /goform/setLinksysIpv6. La manipolazione dell'argomento _6rd_prefix/_6rd_prefix_len provoca un'iniezione di comandi OS. L'attacco può essere eseguito da remoto. L'exploit è stato reso pubblico e potrebbe 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 found in Linksys E1700 1.0.0.4.003. This affects the function setLinksysIpv6 of the file /goform/setLinksysIpv6. The manipulation of the argument _6rd_prefix/_6rd_prefix_len results in os command injection. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?
Sfruttando questa vulnerabilità, un attaccante remoto potrebbe ottenere il controllo completo del router, compromettendo l'intera rete aziendale. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi critici e all'utilizzo del dispositivo per ulteriori attacchi.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
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 criticità della vulnerabilità e la disponibilità pubblica dell'exploit, isolare immediatamente il dispositivo Linksys E1700 su un segmento di rete dedicato. Limitare l'accesso alla sua interfaccia di gestione solo da reti interne fidate e, se possibile, rimuoverlo dall'esposizione diretta a Internet per prevenire attacchi remoti.

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

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

Probabilità di Sfruttamento: high

Termini Alternativi: Command injection

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

Probabilità di Sfruttamento: high

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

Approfondisci su VulnX

CVE-2026-108895 - CVSS 9.9 (CRITICA)

È stata identificata una vulnerabilità in Linksys E1700 1.0.0.4.003. L'elemento interessato è la funzione setDMZ del file /goform/setDMZ. L'esecuzione di una manipolazione dell'argomento MAC_addr può portare a un'iniezione di comandi OS. L'attacco può essere eseguito da remoto. L'exploit è stato reso disponibile al pubblico e potrebbe essere utilizzato per attacchi. Il fornitore è stato contattato tempestivamente riguardo a questa divulgazione, ma non ha risposto in alcun modo.

Descrizione Originale (EN): A weakness has been identified in Linksys E1700 1.0.0.4.003. The affected element is the function setDMZ of the file /goform/setDMZ. Executing a manipulation of the argument MAC_addr can lead to os command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?
Un attaccante remoto può ottenere il controllo completo del router, compromettendo l'intera rete aziendale. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi critici e all'utilizzo del dispositivo come punto di accesso per ulteriori attacchi interni.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Poiché non è disponibile una patch, implementare un firewall a monte del router Linksys E1700 per ispezionare e filtrare il traffico. Configurare regole che blocchino specificamente le richieste HTTP dirette alla funzione '/goform/setDMZ' o che contengano argomenti 'MAC_addr' anomali, impedendo così l'iniezione di comandi OS.

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

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

Probabilità di Sfruttamento: high

Termini Alternativi: Command injection

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

Probabilità di Sfruttamento: high

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

Approfondisci su VulnX

CVE-2026-108894 - CVSS 9.9 (CRITICA)

È stata scoperta una vulnerabilità di sicurezza in Linksys E1700 1.0.0.4.003. Interessata è la funzione addStaticRoute del file /goform/addStaticRoute del componente Static Route Handler. La manipolazione dell'argomento staticRoute_IP_setting/staticRoute_Netmask_setting/staticRoute_Gateway_setting/staticRoute_Metric_setti può portare a un'iniezione di comandi OS. È possibile sfruttare l'attacco da remoto. L'exploit è stato reso pubblico e può essere utilizzato per attacchi. Il fornitore è stato contattato tempestivamente riguardo a questa divulgazione, ma non ha risposto in alcun modo.

Descrizione Originale (EN): A security flaw has been discovered in Linksys E1700 1.0.0.4.003. Impacted is the function addStaticRoute of the file /goform/addStaticRoute of the component Static Route Handler. Performing a manipulation of the argument staticRoute_IP_setting/staticRoute_Netmask_setting/staticRoute_Gateway_setting/staticRoute_Metric_setting results in os command injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?
Sfruttando questa vulnerabilità, un attaccante remoto può ottenere il controllo completo del router e della rete aziendale. Ciò permetterebbe il furto di dati sensibili, l'interruzione dei servizi e l'esecuzione di attacchi mirati all'interno della rete.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Data la gravità della vulnerabilità e l'assenza di una patch, è fondamentale isolare il router Linksys E1700 su un segmento di rete dedicato e strettamente controllato. Implementare rigorosi controlli di accesso e limitare il traffico in entrata e in uscita da questo segmento solo a quanto strettamente necessario, per contenere il potenziale impatto di un'eventuale compromissione.

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

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

Probabilità di Sfruttamento: high

Termini Alternativi: Command injection

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

Probabilità di Sfruttamento: high

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

Approfondisci su VulnX

CVE-2026-108893 - CVSS 9.9 (CRITICA)

È stata identificata una vulnerabilità in Linksys E1700 fino alla versione 1.0.0.4.003. Questo problema riguarda la funzione setVlan del file /goform/setVlan. Una manipolazione dell'argomento vlan_set porta a un overflow del buffer basato su stack. L'attacco può essere eseguito da remoto. L'exploit è pubblicamente disponibile e potrebbe 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 identified in Linksys E1700 up to 1.0.0.4.003. This issue affects the function setVlan of the file /goform/setVlan. Such manipulation of the argument vlan_set leads to stack-based buffer overflow. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.

Cosa può succedere?

Sfruttando questa vulnerabilità critica, un aggressore remoto può ottenere il controllo completo dei router Linksys interessati, compromettendo l'intera rete aziendale. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi di rete essenziali e all'uso dei dispositivi compromessi per lanciare ulteriori attacchi.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Limitare l'accesso all'interfaccia amministrativa del Linksys E1700 esclusivamente da reti interne fidate, preferibilmente tramite VPN o VLAN di gestione dedicate. Assicurarsi che l'interfaccia di gestione non sia esposta direttamente a Internet, riducendo drasticamente la superficie di attacco remota.

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

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

Probabilità di Sfruttamento: high

Termini Alternativi: Buffer Overflow, buffer overrun, memory safety

---

121: **Stack-based Buffer Overflow**

Probabilità di Sfruttamento: high

Termini Alternativi: Stack Overflow, Stack Buffer Overflow

Approfondisci su VulnX

CVE-2026-109390 - CVSS 9.8 (CRITICA)

AnyDesk prima della versione 8.0.3 consente a attori remoti non autenticati di eseguire codice arbitrario tramite un overflow del buffer basato su heap, come dimostrato su Linux per l'esecuzione di comandi come root senza che la vittima approvi il controllo del desktop. Nel gestore dei pacchetti di stream per la modalità 5 nel protocollo di sessione, un valore di lunghezza del payload non viene convalidato.

Descrizione Originale (EN): AnyDesk before 8.0.3 allows unauthenticated remote attackers to execute arbitrary code via a heap-based buffer overflow, as demonstrated on Linux for command execution as root without the victim approving desktop control. In the stream packet handler for mode 5 in the session protocol, a payload length value is not validated.

Cosa può succedere?
Un attaccante remoto non autenticato potrebbe ottenere il controllo completo dei sistemi aziendali che utilizzano AnyDesk vulnerabile. Questo consentirebbe il furto di dati sensibili, l'interruzione dei servizi critici e la potenziale diffusione dell'attacco ad altri sistemi della rete.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:
Implementare una rigorosa segmentazione di rete per isolare le istanze di AnyDesk. Assicurarsi che il servizio sia accessibile solo da reti interne fidate o tramite VPN, limitando l'esposizione diretta a reti non controllate per mitigare il rischio di esecuzione di codice arbitrario da parte di attori remoti non autenticati.

CVSS Metrics

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

CWE - Common Weakness Enumeration

130: **Improper Handling of Length Parameter Inconsistency**

Termini Alternativi: length manipulation, length tampering

Approfondisci su VulnX

CVE-2026-66086 - CVSS 9.8 (CRITICA)

Nello stack OTA del modem, è presente un possibile overflow del buffer basato su stack a causa di una convalida inadeguata delle informazioni di pianificazione nei messaggi SIB1. Ciò potrebbe portare a un'esecuzione remota di codice o a un denial of service senza richiedere privilegi di esecuzione aggiuntivi.

Descrizione Originale (EN): In the modem OTA stack, there is a possible stack-based buffer overflow due to improper validation of scheduling information in SIB1 messages. This could lead to remote code execution or denial of service with no additional execution privileges needed.

Cosa può succedere?

Gli attaccanti potrebbero ottenere il controllo completo dei sistemi o dispositivi interessati. Ciò potrebbe portare al furto di dati sensibili, all'interruzione dei servizi critici o al blocco operativo dell'azienda.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	0.46% (Percentile: 0.38)
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Per mitigare il rischio di questa vulnerabilità critica, isolate i modem o i sistemi che elaborano i messaggi SIB1 in un segmento di rete dedicato e strettamente controllato. Questo aiuterà a limitare l'esposizione a traffico potenzialmente malevolo e a contenere l'impatto di un eventuale sfruttamento, anche tramite l'applicazione di regole di filtraggio rigorose ai confini del segmento.

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

Approfondisci su VulnX

CVE-2026-9191 - CVSS 9.6 (CRITICA)

Progress MarkLogic Server 12.x rilasci prima di 12.1.0 e le versioni 11.x prima di 11.3.7 non isolano in modo sufficiente il codice fornito dall'utente eseguito tramite determinati percorsi di valutazione REST e XDBC dallo stato della richiesta HTTP, della risposta e della sessione. Un attaccante in grado di eseguire codice attraverso un percorso interessato potrebbe compiere azioni non autorizzate o compromettere una sessione autenticata.

Descrizione Originale (EN): Progress MarkLogic Server 12.x releases before 12.1.0 and 11.x releases before 11.3.7 do not sufficiently isolate user-supplied code executed through certain REST and XDBC evaluation paths from HTTP request, response, and session state. An attacker able to execute code through an affected path could perform unauthorized actions or compromise an authenticated session.

Cosa può succedere?

Un attaccante può eseguire azioni non autorizzate, come il furto di dati sensibili o la manipolazione di informazioni aziendali critiche. Questo potrebbe portare alla compromissione completa del sistema MarkLogic, causando interruzioni dei servizi, perdite finanziarie significative e gravi danni alla reputazione aziendale.

Punteggio CVSS:	9.6 (CRITICA)
EPSS:	N/A
Pubblicata:	12/10/2026
Modificata:	12/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

Raccomandazione di Sicurezza:

Implementare una rigorosa segmentazione di rete per isolare le istanze di MarkLogic Server, in particolare quelle che espongono i percorsi di valutazione REST e XDBC. Limitare l'accesso a tali percorsi solo a sistemi e utenti strettamente autorizzati. Ciò ridurrà drasticamente la superficie di attacco e la probabilità di sfruttamento di questa vulnerabilità critica.

CVSS Metrics

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

CWE - Common Weakness Enumeration

346: **Origin Validation Error**

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-2015-3306 KEV

CVSS: 10.0/10 **EPSS:** 99.5% **Target:** Unknown **Rischio:** 10.0/10

Perché è una minaccia prioritaria:
Questo rappresenta una minaccia critica perché ha un punteggio CVSS di 10.0, una probabilità di exploit del 99.5% ed è attivamente sfruttato, come confermato dalla sua inclusione nel CISA KEV.

Minaccia #2: CVE-2016-3081 KEV

CVSS: 8.1/10 **EPSS:** 96.1% **Target:** Unknown **Rischio:** 8.7/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché ha un'altissima probabilità di essere sfruttata (EPSS 96.1%), è attivamente utilizzata dagli attaccanti (CISA KEV) e ha un grave impatto (CVSS 8.1/10).

Minaccia #3: CVE-2015-5477 KEV

CVSS: 7.5/10 **EPSS:** 99.4% **Target:** Unknown **Rischio:** 8.5/10

Perché è una minaccia prioritaria:
Questa rappresenta una minaccia critica perché è attivamente sfruttata (CISA KEV) e presenta una probabilità di exploit estremamente alta (EPSS 99.4%), rendendola un bersaglio facile e immediato.

5.1 EPSS Elevato (>95%)

Impossibile recuperare i dettagli delle vulnerabilità.

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