VulnX

studio consi
sicurezza digitale

Report di Threat Intelligence

Periodo: Settimanale

26/10/2026 - 02/11/2026

Generato il: **02/11/2026 06:01**

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 10

4 Vulnerabilità Critiche **37**

5 Top 3 Minacce della Settimana **37**
5.1 EPSS Elevato (>95%) 38
5.2 Raccomandazioni 39
5.3 Risorse Aggiuntive 39

1 Sommario Esecutivo

INDICATORE DI RISCHIO SETTIMANALE

ALTO

Rilevate 22 vulnerabilità critiche e 0 exploit attivi.

Metrica	Valore
Totale CVE	**362**
Critiche	**22**
Alte	**81**
EPSS >50%	**0**
KEV	**0**

1.1 Statistiche del Periodo

Panoramica del Periodo Analizzato:

Metrica	Valore	%
Volume di Pubblicazione		
CVE Pubblicate	**362**	–
CVE Modificate	7,660	–
Distribuzione Severità (CVSS)		
Critiche (9.0-10.0)	**22**	7.2%
Alte (7.0-8.9)	**81**	26.6%
Medie (4.0-6.9)	177	58.0%
Basse (0.1-3.9)	25	8.2%
Indicatori di Rischio		
KEV (Exploit Attivi)	**0**	0.0%
EPSS Elevato (>50%)	0	0.0%

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

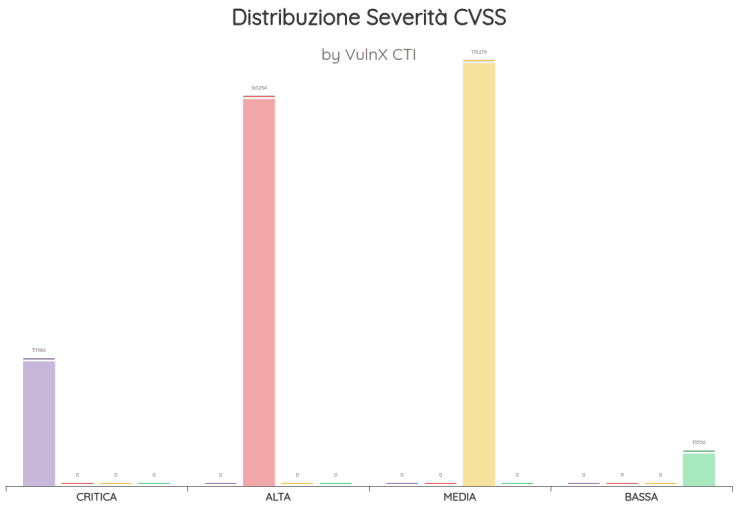
1.2 Panoramica Database (Storico Completo)

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

- **CVE Totali nel Database:** 414,225
- **KEV Totali (Vulnerabilità con Exploit Noti):** 1,758
- **CWE Totali Catalogate:** 969
- **CPE Totali Monitorati:** 2,533,821

Severità	Conteggio	Percentuale
CRITICA	51,986	12.9%
ALTA	161,254	40.0%
MEDIA	176,219	43.7%
BASSA	13,556	3.4%

Tabella 1: *Distribuzione per Severità*




Evoluzione Temporale delle CVE
by VulnX CTI
100,000
80,000
60,000
40,000
20,000
0
CVE
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026

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:

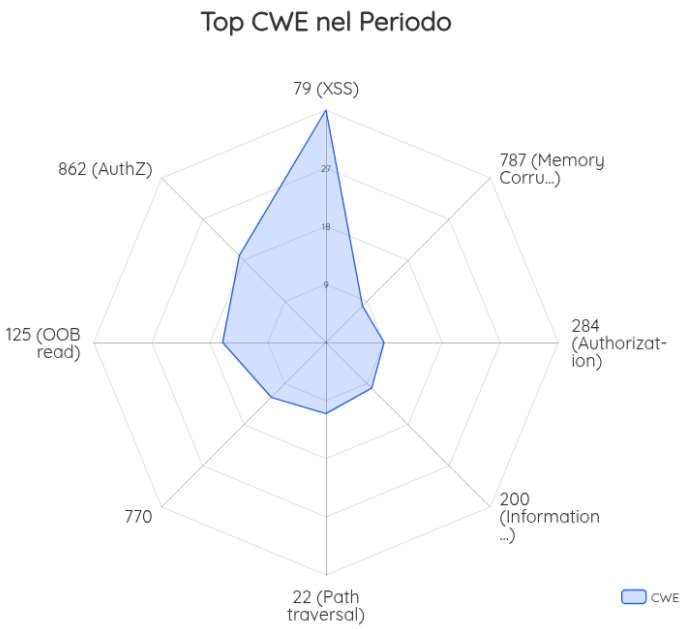


Figura 1: *Distribuzione Top CWE - Grafico Radar*

3.2 Analisi Approfondita delle Debolezze (CWE)

Le debolezze più comuni con raccomandazioni di difesa.

22

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

▶ **Occorrenze:** 11

200

Exposure of Sensitive Information to an Unauthorized Actor

▶ **Occorrenze:** 10

287

Improper Authentication

▶ Occorrenze: 6

321

Use of Hard-coded Cryptographic Key

▶ Occorrenze: 4

409

Improper Handling of Highly Compressed Data (Data Amplification)

▶ Occorrenze: 4

209

Generation of Error Message Containing Sensitive Information

▶ Occorrenze: 4

3.3 CVE del Periodo Analizzato

Trovate **362** CVE nel periodo. Per approfondire tutte le vulnerabilità identificate si rimanda alla piattaforma VulnX. Mostrando le prime **25** CVE:

CVE-2026-115905 - CVSS 10.0 (CRITICA)

zip is a zip library for Rust that supports reading and writing simple ZIP files. Through 9.0.4, ZipArchive treats Central Directory File Header filenames as authoritative while ZipStreamReader extracts using Local File Header filenames without reconciling the duplicate metadata in src/read/stream.rs. A crafted archive can therefore appear benign to a component that inspects the central directory but cause a streaming extractor to write a different attacker-selected path and content, potentially overwriting files used by a downstream service. This issue is fixed in version 9.0.5.

Punteggio CVSS:	10.0 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

20: **Improper Input Validation**

Probabilità di Sfruttamento: high

436: **Interpretation Conflict**

Approfondisci su VulnX

CVE-2026-110720 - CVSS 9.9 (CRITICA)

Consul-k8s versions 0.42.0 and later are vulnerable to a cross-namespace authorization bypass in component ACL binding rules that may allow an attacker to obtain elevated Consul privileges. This vulnerability (CVE-2026-110720) is fixed in consul-k8s 2.1.0 and 1.8.18.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	27/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

863: **Incorrect Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Approfondisci su VulnX

CVE-2026-102649 - CVSS 9.9 (CRITICA)

Burrito is a Terraform Automation Collaboration Software (TACoS) Kubernetes operator. Prior to 0.13.0, ‘POST /api/webhook‘ accepts unsigned GitHub and GitLab events when a ‘TerraformRepository‘’s credentials omit ‘webhookSecret‘ or set it to an empty value, including credentials configured for git authentication and polling. ‘Credential.WebhookSecret‘ is optional, and ‘go-playground/webhooks‘ skips signature or token verification when the secret is empty. Anyone who can reach ‘burrito-server‘’s endpoint and knows a tracked repository’s URL can forge events to create or delete ‘TerraformPullRequest‘ custom resources with attacker-chosen ‘Branch‘, ‘Base‘, and ‘ID‘ fields. For GitHub ‘pull_request‘ events, the controller fetches changed files using the real pull request number but does not cross-check the payload’s branch against that pull request. Pairing a real, existing pull request number with an unrelated existing branch in the same repository can therefore cause an unauthorized ‘terraform plan‘ for affected layers using the operator’s stored git and cloud credentials. Code analysis also indicates that the resulting plan can be posted to the real pull request’s comment thread, exposing and misattributing another branch’s infrastructure changes. Auto-apply is disabled for these temporary layers, so this vulnerability alone cannot force a ‘terraform apply‘; plan-time provider and data-source code execution depends on the selected branch’s contents. This issue is fixed in version 0.13.0.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

306: **Missing Authentication for Critical Function**

Probabilità di Sfruttamento: high

863: **Incorrect Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Approfondisci su VulnX

CVE-2026-115188 - CVSS 9.9 (CRITICA)

An unrestricted file upload vulnerability exists in the campaign import feature of Mautic 7. When processing an uploaded campaign archive, the application copies the bundled asset files into a publicly accessible media directory without restricting their file names or types. An authenticated user with permission to create campaign imports can exploit this through the user interface or the API (/api/campaigns/import) to place arbitrary files, including server-side scripts, in the web root. Administrator privileges are not required. On web servers that honor per-directory configuration, such as the default Apache setup of the official Mautic Docker image, this leads to remote code execution with the privileges of the web server user, including access to the Mautic configuration, application secrets, and contact data.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Code Injection

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

Probabilità di Sfruttamento: medium

Termini Alternativi: Unrestricted File Upload

Approfondisci su VulnX

CVE-2026-116231 - CVSS 9.9 (CRITICA)

A security flaw has been discovered in Oray Pugongying X5 Pro 7.6.1. The impacted element is an unknown function of the component Ser2net. Performing a manipulation of the argument regmsg results in crlf injection. It is possible to initiate the attack remotely. 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.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

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

Probabilità di Sfruttamento: high

93: **Improper Neutralization of CRLF Sequences ('CRLF Injection')**

Approfondisci su VulnX

CVE-2026-116232 - CVSS 9.9 (CRITICA)

A weakness has been identified in Oray Pugongying X5 Pro 7.6.1. This affects the function snmp_set of the component SNMP Handler. Executing a manipulation of the argument info.community can lead to crlf injection. It is possible to launch the attack 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.

Punteggio CVSS:	9.9 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

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

Probabilità di Sfruttamento: high

93: **Improper Neutralization of CRLF Sequences ('CRLF Injection')**

Approfondisci su VulnX

CVE-2026-112346 - CVSS 9.8 (CRITICA)

OpenHands Software Agent SDK before 1.52.0 contains an unauthenticated remote code execution vulnerability where the DockerWorkspace and Apptainer workspace launchers bind the sandbox agent server to all network interfaces (0.0.0.0) with an empty session_api_keys list, disabling authentication by default. Attackers who can reach the published container port can send unauthenticated HTTP and WebSocket requests to execute arbitrary shell commands as root in the sandbox, access the mounted workspace, and read plaintext secrets from the secrets store.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

1327: **Binding to an Unrestricted IP Address**

Approfondisci su VulnX

CVE-2026-10757 - CVSS 9.8 (CRITICA)

There is a SQL injection vulnerability in Esri ArcGIS Server versions 12.1 and earlier on Windows and Linux that may allow a remote attacker with privileges to access the service (which could, depending on the service being configured in a non-default access configuration “public”, include an anonymous attacker) to issue database specific functions that should not be allowed. A patch is provided for ArcGIS Server software in General Availability and Extended support status, which includes versions 12.1, 12.0, 11.5, 11.3, and 11.1. Other versions are in mature or retired status, which are not patch eligible. Users working with unlisted versions are advised to upgrade and apply the patch.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	27/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Termini Alternativi: SQL injection, SQLi

Approfondisci su VulnX

CVE-2026-65184 - CVSS 9.8 (CRITICA)

The root-privileged ‘wsserver‘ terminal-bridge daemon builds a shell command from client-supplied WebSocket fields and passes it to ‘system()‘ and ‘popen()‘ without quoting, escaping, or character-set validation. The daemon’s public-key session path performs no appliance-session check.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

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

Approfondisci su VulnX

CVE-2026-59106 - CVSS 9.8 (CRITICA)

A security vulnerability has been identified in the WolfProt interface implementation. Insufficient neutralization of user-controlled input could allow an unauthenticated attacker with network access to a vulnerable service to execute operating-system commands with the privileges of the affected application service.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

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

Approfondisci su VulnX

CVE-2026-59107 - CVSS 9.8 (CRITICA)

A security vulnerability has been identified in the vSolution Matrix file sharing feature. A shared cryptographic trust configuration could allow an attacker who obtains the matching private key to authenticate to an affected device via SSH as root. This vulnerability affects only devices configured as a vSolution Matrix main/master station with the file sharing feature enabled.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

797: **Only Filtering Special Elements at an Absolute Position**

Approfondisci su VulnX

CVE-2026-116485 - CVSS 9.8 (CRITICA)

danmu_api before 1.21.7 contains an authentication bypass vulnerability that allows unauthenticated attackers to modify server environment configuration when the default TOKEN is used and ADMIN_TOKEN is unset. Attackers can send POST requests to /api/env/set, /api/env/add, or /api/env/del to set ADMIN_TOKEN, lock out operators, redirect OTHER_SERVER or PROXY_URL for SSRF, and trigger redeployment.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

Approfondisci su VulnX

CVE-2026-107092 - CVSS 9.8 (CRITICA)

NexoPOS v6.2.4 is vulnerable to Directory Traversal via the api/update endpoint.

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

Approfondisci su VulnX

CVE-2026-107656 - CVSS 9.8 (CRITICA)

An authentication bypass using an alternate path or channel vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.6, FortiSandbox 4.4.0 through 4.4.9, FortiSandbox 4.2 all versions, FortiSandbox PaaS 5.0.0 through 5.0.6, FortiSandbox PaaS 4.4 all versions, FortiSandbox PaaS 4.2 all versions may allow attacker to execute unauthorized code or commands via crafted HTTP requests

Punteggio CVSS:	9.8 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	27/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

288: **Authentication Bypass Using an Alternate Path or Channel**

Approfondisci su VulnX

CVE-2026-93328 - CVSS 9.3 (CRITICA)

Path Traversal and Missing Authorization in cloud-storage source in Google Cloud MCP Toolbox for Databases (googleapis/mcp-toolbox) versions 1.2.0 through 1.4.0 allows an unauthenticated remote attacker to exfiltrate host files to external Google Cloud Storage buckets and overwrite arbitrary local files via crafted tool invocation parameters.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

Termini Alternativi: Path traversal, Directory traversal, Path transversal

---

862: **Missing Authorization**

Probabilità di Sfruttamento: high

Termini Alternativi: AuthZ

Approfondisci su VulnX

CVE-2026-110475 - CVSS 9.3 (CRITICA)

This vulnerability exists in the CreditNirvana Collections Platform due to improper authentication and authorization controls at the platform login service. An unauthenticated remote attacker could exploit this vulnerability by manipulating authentication requests and accessing APIs without a valid authenticated session on the targeted system. Successful exploitation of this vulnerability could allow the attacker to enumerate platform users, establish sessions as arbitrary users including administrative users, access and modify sensitive information with the privileges of the impersonated user.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

1390: **Weak Authentication**

Approfondisci su VulnX

CVE-2026-77055 - CVSS 9.3 (CRITICA)

boneIO black_debian_images gives the boneio service account excessive privileges, including full passwordless sudo access and membership in the docker group. A local attacker who compromises the boneio user can use these privileges to escalate to root. This issue was fixed in version 1.6.0: the image removes the sudoers rule and the docker group membership when it is sealed, and devices already in the field have both removed by migrations shipped with boneio 1.6.0 and applied on first start after the upgrade. Privileged operations now go through helpers that accept only a fixed set of commands, with migrations verified against Ed25519 signatures.

Punteggio CVSS:	9.3 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

266: **Incorrect Privilege Assignment**

Approfondisci su VulnX

CVE-2026-116214 - CVSS 9.1 (CRITICA)

MacCMS v10 before 2026.1000.4054 contains an authentication bypass vulnerability that allows unauthenticated attackers to reset any member's password because check_msg() never compares msg_to. Attackers can request a recovery code to their own mailbox via user/findpass_msg, then submit it to user/findpass_reset with the victim's email or phone to take over the account.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

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

Probabilità di Sfruttamento: high

Approfondisci su VulnX

CVE-2026-115693 - CVSS 9.1 (CRITICA)

Improper Certificate Validation vulnerability in hackney_ssl in benoitc hackney allows an on-path attacker to impersonate a server pinned to a private certificate authority via a certificate chain that ends in a publicly trusted root. hackney adds {partial_chain, fun hackney_ssl:partial_chain/1} to every verify_peer configuration. The callback returns any certificate in the peer chain whose public key matches a root in the bundled certifi store as the trust anchor, and OTP honours that callback over the configured cacerts. hackney_ssl:merge_ssl_opts/3 kept the callback when the caller replaced the trust store with cacerts or cacertfile in ssl_options, so a connection pinned to a private CA still accepted any chain that carried a publicly trusted root. The hostname check still applies, so the attacker needs a publicly trusted certificate for the pinned hostname. This issue affects hackney: from 1.24.0 before 4.9.0.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

295: **Improper Certificate Validation**

Approfondisci su VulnX

CVE-2026-116235 - CVSS 9.1 (CRITICA)

A flaw has been found in Oray Pugongying X5 Pro 7.6.1. Affected by this vulnerability is an unknown functionality of the component L2TP Authentication. This manipulation of the argument Username causes crlf injection. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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:** high

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

93: **Improper Neutralization of CRLF Sequences ('CRLF Injection')**

Approfondisci su VulnX

CVE-2026-116234 - CVSS 9.1 (CRITICA)

A vulnerability was detected in Oray Pugongying X5 Pro 7.6.1. Affected is an unknown function of the file /etc/ipsec.conf of the component IPsec Policy Handler. The manipulation of the argument secproto results in crlf injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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:** high

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

93: **Improper Neutralization of CRLF Sequences ('CRLF Injection')**

Approfondisci su VulnX

CVE-2026-116233 - CVSS 9.1 (CRITICA)

A security vulnerability has been detected in Oray Pugongying X5 Pro 7.6.1. This impacts an unknown function of the component Dnsmasq. The manipulation of the argument rent_time leads to crlf injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

Punteggio CVSS:	9.1 (CRITICA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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:** high

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: high

93: **Improper Neutralization of CRLF Sequences ('CRLF Injection')**

Approfondisci su VulnX

CVE-2026-105608 - CVSS 8.8 (ALTA)

HashiCorp Consul and Consul Enterprise are vulnerable to an authorization bypass in service mesh proxy registration. This may allow a user with service write permission to apply Envoy escape-hatch configuration without the required mesh write permission. This vulnerability (CVE-2026-105608) is fixed in Consul Community Edition 2.1.0 and Consul Enterprise 2.1.0 and 1.21.19.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

178: **Improper Handling of Case Sensitivity**

Approfondisci su VulnX

CVE-2026-115748 - CVSS 8.8 (ALTA)

UNSUPPORTED WHEN ASSIGNED Authorization bypass in Apache Vysper, all versions. Apache Vysper is an XMPP (Jabber) server library. Its XEP-0077 (In-Band Registration) implementation is missing an authentication check, allowing any authenticated user to compromise other accounts. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

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

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-2026-77059 - CVSS 8.8 (ALTA)

boneIO Black contains a TOCTOU race condition in the create_timedatectl_sudoers_file() function in boneio/webui/routes/timezone_sudoers.py. The function writes sudoers rules to a predictable temporary file, validates them, then installs them with root privileges. A local attacker can exploit the race window between validation and installation to substitute malicious content, or use the predictable filename for symlink attacks, resulting in arbitrary sudoers rule injection and local privilege escalation to root. This issue was fixed in version 1.6.0.

Punteggio CVSS:	8.8 (ALTA)
EPSS:	N/A
Pubblicata:	26/10/2026
Modificata:	26/10/2026
KEV (Vulnerabilità Sfruttata):	No
Exploit Disponibili:	No

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

CVSS Metrics

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

CWE - Common Weakness Enumeration

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

Probabilità di Sfruttamento: medium

Termini Alternativi: TOCTTOU, TOCCTOU

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-2026-115905

CVSS: 10.0/10 **EPSS:** 0.0% **Target:** Unknown **Rischio:** 6.0/10

Minaccia #2: CVE-2026-110720

CVSS: 9.9/10 **EPSS:** 0.0% **Target:** Unknown **Rischio:** 5.9/10

Minaccia #3: CVE-2026-102649

CVSS: 9.9/10 **EPSS:** 0.0% **Target:** Unknown **Rischio:** 5.9/10

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