Daily brief, Monday, November 9, 2026

Nov 8, 7:00 PM to Nov 9, 7:00 PM ET

Generated Nov 9, 2026, 10:36 PM ET

2	0	4	22	116	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 breaking, 1 emerging, 4 with new public exploit code, 22 new critical CVEs, 116 ransomware posts.

Breaking 2

OpenBSD OpenSSH: Auth bypass / access control (2 CVEs)

- 14 posts from 12 independent sources in 48 h
- rising: 10 posts in the last 24 h
- OpenSSH: very widely used in large enterprises
- auth bypass / access control
- public exploit code
- Cloudflare Zero Wire: needs attention

CVEs: CVE-2026-123158, CVE-2026-98432

SonicWall SonicOS

- 13 posts from 10 independent sources in 48 h
- SonicWall: widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)

CVEs: CVE-2026-19868

Emerging 1

Critical bugs in widely used enterprise tech, not spreading widely yet.

Node2Shell · Node.js

- 4 posts from 4 independent sources in 48 h
- Node.js: very widely used in large enterprises
- exploited in the wild (CISA KEV)
- public exploit code
- Cloudflare Zero Wire: needs attention

CVEs: CVE-2026-111497

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code 4

9.3 **CVE-2026-116606** Barracuda Networks Barracuda Email Security Gate… NUCLEI TEMPLATE DETECTION

Unauthenticated remote attacker bypasses auth in Barracuda Email Security Gateway before 9.4.0.030 and imports a crafted backup, modifying global configuration.

9.1 **CVE-2026-118066** Latepoint Appointment Booking Plugin – LatePoint |… NUCLEI TEMPLATE DETECTION

Authentication bypass in the LatePoint appointment booking plugin for WordPress, through version 5.7.6, lets attackers take over user accounts.

8.1 **CVE-2026-118267** Peterschulznl WP Data Access – App Builder for Ta… NUCLEI TEMPLATE DETECTION

Attackers escalate privileges in the WP Data Access WordPress plugin through version 5.5.89 via write endpoints that enforce incorrect authorization.

10.0 **CVE-2025-49387** Add-Ons.Org Drag and Drop File Upload for Element… NUCLEI TEMPLATE DETECTION

CVE published Aug 28, 2025

Unrestricted Upload of File with Dangerous Type vulnerability in add-ons.org Drag and Drop File Upload for Elementor Forms drag-and-drop-file-upload-for-elementor-forms allows Upload a Web Shell to a Web Server.This issue affects Drag and Drop File Upload for

1 older CVE (published more than 7 days earlier) with new exploit code, below the bar (CVSS under 9, not widely used enterprise tech):
CVE-2026-16062 (6.6)

New critical CVEs 22

10.0 **CVE-2026-115252** Unknown Confection WordPress Cable

Unauthenticated attackers execute arbitrary PHP code on servers running The Confection WordPress Cable plugin 0.4.0-0.4.7 via unchecked settings saves.

9.8 **CVE-2026-115213** Unknown EASY-JS-WPAPI Client HANDLE for the WordPress REST-API

Unauthenticated attackers can obtain administrator credentials stored by the EASY-JS-WPAPI Client HANDLE WordPress plugin through version 2.0.

9.8 **CVE-2026-125384** Go2ismail Asp.Net-Core-Inventory-Order-Management-System

INDOTALENT WHMS before 10.20261109 contains a default credentials vulnerability that allows unauthenticated attackers to gain administrator access because UserAdminSeeder creates admin@root.com with password 123456. Attackers can log in with these credentials,

10.0 **CVE-2026-124580** Chengdu Feiyuxing Technology VW2100

Command injection via the extend argument of the Weixin Auth Endpoint lets attackers run OS commands on Chengdu Feiyuxing VW2100 and VEC10GP 1.0 devices.

10.0 **CVE-2026-110468** Fundacja Widzialni WidzialniCMS

Unauthenticated attacker can upload arbitrary files to any server location in WidzialniCMS via /panel/controllers/save_photo.php.

10.0 **CVE-2026-110469** Fundacja Widzialni WidzialniCMS

Unauthenticated attackers can upload arbitrary files to any server location through /panel/upload.php in WidzialniCMS by Fundacja Widzialni.

9.9 **CVE-2026-124585** Chengdu Feiyuxing Technology VW2100

An attacker can inject OS commands via the mac argument in the web administration interface of Chengdu Feiyuxing VW2100 and VEC10GP 1.0 firmware.

9.9 **CVE-2026-123800** Supertokens supertokens-core

An attacker can bypass authorization checks on multitenancy create and update operations in SuperTokens Core from 6.0.0 until the fixed releases, including 6.0.24 and 7.0.23.

9.8 **CVE-2026-124560** D-Link DIR-878

Remote attacker triggers a heap-based buffer overflow via the uid argument of GetCAPTCHAsetting in the D-Link DIR-878 1.20B05 HNAP handler; a public exploit exists.

9.8 **CVE-2026-115237** Unknown Grand Job

Unauthenticated attackers can set the password of any account, including administrators, via the Grand Job WordPress plugin through 1.2.1, fully taking over the site.

9.8 **CVE-2026-123751** Unknown WP Duplicate

Unauthenticated attackers can upload arbitrary files to the WP Duplicate WordPress plugin through 1.1.11, achieving remote code execution on the server.

9.8 **CVE-2026-124577** Intelbras SG 2404 PoE L2+

A remote attacker can bypass authentication in the Web Management Interface of Intelbras SG 2404 PoE L2+ 1.00.70/1.00.72 via the /EXCU_SHELL file.

9.8 **CVE-2026-124079** rConfig rConfig Core

rConfig Core 8.0.0 before 8.2.19 and rConfig Pro before 8.4.1 contain a deserialization of untrusted data vulnerability that allows unauthenticated network attackers to execute arbitrary code by pushing a crafted serialized job onto the Redis-backed Laravel Ho

9.8 **CVE-2026-119756** Arendst Tasmota
Unauthenticated attackers on the local network can corrupt heap memory in Tasmota through 16.0.0 by sending crafted Device Groups messages over UDP port 4447.

9.8 **CVE-2026-123270** Redpanda Data Connect
Unauthenticated remote code execution in Redpanda Connect 4.39-4.110 streams mode via the management HTTP API on port 4195, which has auth disabled by default.

9.8 **CVE-2026-125120** Automattic mongoose
Mongoose countDocuments() bypasses the sanitizeFilter defense, letting attackers inject MongoDB query selectors in Mongoose before 6.13.11, 7.8.12, 8.24.3, and 9.9.2.

9.5 **CVE-2026-123870** Eclipse Foundation otterdog
Unauthenticated network attackers can inject code via GitHub webhook JSON evaluated by eval() in Eclipse otterdog when GITHUB_WEBHOOK_SECRET is unset or empty.

9.3 **CVE-2026-113363** NEC WebSAM WinShare
A remote unauthenticated attacker can execute arbitrary commands with SYSTEM privileges in NEC WebSAM WinShare 7.2.0 through 7.7.2 on Windows via crafted network packets.

9.3 **CVE-2026-113364** NEC WebSAM WinShare
A remote unauthenticated attacker can execute arbitrary code as SYSTEM via a crafted packet with a malformed data size in NEC WebSAM WinShare on Windows.

9.3 **CVE-2026-104989** Chaos Software V-Ray Swarm
Unauthenticated remote attackers can run arbitrary code in V-Ray Swarm through 2.0.19 via unsafe library search paths in its package upload feature.

2 more critical CVEs in this window: see the dashboard

Ransomware

116

116 victims posted to leak sites. Most active: n0n (66), climax (14), vortex (9), krybit (5), byod (3).

Financial services hit: Company #196 (n0n), Company #194 (n0n), Company #190 (n0n), Company #186 (n0n), Company #187 (n0n), Company #182 (n0n), Company #177 (n0n), Company #176 (n0n), Company #169 (n0n), Company #162 (n0n).

New data breaches

No new breaches published.

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.