Daily brief, Sunday, November 8, 2026

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

Generated Nov 8, 2026, 7:59 PM ET

4	0	0	21	16	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 breaking, 2 emerging, 21 new critical CVEs, 16 ransomware posts.

Breaking 4

SonicWall SonicOS

- 25 posts from 20 independent sources in 48 h
- SonicWall: widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- official advisory

CVEs: CVE-2026-19868

PHP2Shell · PHP

- 12 posts from 11 independent sources in 48 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- reports of exploitation in the wild
- named threat actor activity

OpenBSD OpenSSH: Auth bypass / access control

- 14 posts from 11 independent sources in 48 h
- OpenSSH: very widely used in large enterprises
- auth bypass / access control
- public exploit code
- Cloudflare Zero Wire: needs attention

CVEs: CVE-2026-123158

Microsoft Paint: Memory corruption

- 7 posts from 7 independent sources in 48 h
- Windows: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code
- official advisory

CVEs: CVE-2026-83844

Emerging 2

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

Node2Shell · Node.js

- 3 posts from 3 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

WordPress Foundation WordPress: Code / command injection

- 3 posts from 3 independent sources in 48 h
- PHP: very widely used in large enterprises
- code / command injection
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-119977

Newly exploited in the wild

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

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

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-2026-12592 (7.5)

New critical CVEs 21

9.8 **CVE-2026-114432** Unknown Contact Form 7
Unauthenticated attackers can upload arbitrary files to sites running the Contact Form 7 WordPress plugin before 6.2.4 via form file fields.

9.8 **CVE-2026-110963** Unknown Userplace
Unauthenticated attackers can create administrator accounts or write arbitrary site options in the Userplace WordPress plugin through 1.2.0, due to a missing authorization check on an AJAX action.

10.0 **CVE-2026-123551** OpenIdentityPlatform OpenAM
Unauthenticated attackers can read live session tokens from OpenAM 14.0.0 before 16.1.4 via the notification WebSocket by bypassing an agent-only check.

9.9 **CVE-2026-124440** Kyverno kyverno
Kyverno before 1.19.2 lets namespace tenants bypass the apiCall clamp via malformed urlPath escapes, reaching cross-namespace and cluster-scoped API requests.

9.9 **CVE-2026-124450** Openemr openemr
Authenticated low-privilege users of OpenEMR before 8.3.0 can traverse paths via fax/sms disposeDocument to read DB credentials and write arbitrary files.

9.9 **CVE-2026-124469** Openemr openemr
Low-privileged authenticated users of OpenEMR before 8.3.0 can inject SQL through the Fee Sheet product warehouse field, which is interpolated into an ORDER BY clause.

9.9 **CVE-2026-107331** IBM DataStage on Cloud Pak for Data
Authenticated remote attackers can read sensitive information via absolute-path traversal in IBM DataStage on Cloud Pak for Data 5.4.0.0.

9.8 **CVE-2026-123549** OpenIdentityPlatform OpenAM
Anonymous attackers can set restricted attributes like group membership during self-registration in OpenAM before 16.1.4, escalating to admin privileges.

9.8 **CVE-2026-123550** OpenIdentityPlatform OpenAM
Authentication bypass in OpenAM before 16.1.4 SAML SP lets unauthenticated remote attackers submit forged unsigned assertions to obtain sessions.

9.8 **CVE-2026-123614** Imgproxy imgproxy
Remote attackers can trigger a heap buffer overflow in imgproxy 4.0.0 before 4.0.16 by submitting a crafted ICO image with a wrapping data_size value.

9.8 **CVE-2026-124427** Craftcms cms
Anonymous GraphQL clients of Craft CMS 5.0.0 to before 5.11.2 can read titles, slugs, and custom fields of out-of-scope entries via prev/next chaining.

9.8 **CVE-2026-124445** Openemr openemr
OpenEMR before 8.4.0 lets attackers replay captured service_auth tokens because consumed tokens are never revoked, and login_pin checks lack rate limiting.

9.8 **CVE-2026-15266** IBM Concert
Attacker gets arbitrary system command execution on the host running IBM Concert versions 1.0 through 3.0.1.1 via command injection.

9.8 **CVE-2026-6715** IBM Concert
IBM Concert 1.0 through 3.0.1.1 allows remote attackers to execute arbitrary OS commands via crafted input that is passed unsanitized into a system command.

9.6 **CVE-2026-109900** Melapress Melapress Role Editor
An attacker can escalate privileges in Melapress Role Editor from n/a through 1.3.0 because of incorrect privilege assignment.

9.3 **CVE-2026-124493** JiHong88 suneditor
SunEditor before 3.4.0 stored XSS: attacker stores entity-encoded HTML in h1-h6 headers that runs JavaScript when editors use document:header mode.

9.3 **CVE-2026-124494** JiHong88 suneditor
Stored XSS in JiHong88 SunEditor before 3.4.0: crafted href values like javascript: bypass the URL sanitizer and execute script in victims' browsers.

9.3 **CVE-2026-114464** IBM Process Mining
Remote attackers can obtain sensitive information from IBM Process Mining versions 2.0.0 through 2.2.1 due to improper access control.

9.1 **CVE-2026-124490** Openemr openemr
OpenEMR before 8.3.0's oe-module-faxsms path traversal lets authenticated attackers read and write arbitrary files, including credentials and source.

9.1 **CVE-2026-101117** IBM WebSphere Extreme Scale
A remote attacker can bypass security restrictions in IBM WebSphere Extreme Scale 8.6.1.0 through 8.6.2.2 due to an improper Content Security Policy configuration.

1 more critical CVEs in this window: see the dashboard

Ransomware 16

16 victims posted to leak sites. Most active: lockbit5 (4), deadlock (4), majinahanashi (3), whitearmor (1), orova (1).

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.