Daily brief, Saturday, October 31, 2026

Oct 30, 8:00 PM to Oct 31, 8:00 PM ET

Generated Nov 6, 2026, 3:23 PM ET

5	0	1	13	15	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 breaking, 1 emerging, 1 with new public exploit code, 13 new critical CVEs, 15 ransomware posts.

Breaking 5

PHP2Shell · PHP

- 166 posts from 64 independent sources in 48 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code
- emergency / unpatched

CVEs: CVE-2026-98432, CVE-2026-109618, CVE-2026-109619, CVE-2026-46300

GitLab: Memory corruption (2 CVEs)

- 33 posts from 25 independent sources in 48 h
- Cisco: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code
- emergency / unpatched

CVEs: CVE-2026-97229, CVE-2026-76418

Node2Shell · Node.js

- 11 posts from 10 independent sources in 48 h
- Node.js: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-111497

Ivanti Connect Secure: Privilege escalation (3 CVEs)

- 9 posts from 7 independent sources in 48 h
- Ivanti: very widely used in large enterprises
- privilege escalation
- exploited in the wild (CISA KEV)
- public exploit code
- official advisory

CVEs: CVE-2026-111357, CVE-2026-118527, CVE-2026-104935

Cisco Catalyst SD-WAN Controller and Manager: Auth bypass / access control

- 7 posts from 6 independent sources in 48 h
- Cisco: very widely used in large enterprises
- auth bypass / access control
- exploited in the wild (CISA KEV)
- public exploit code
- named threat actor activity

CVEs: CVE-2026-20127

Emerging 1

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

VMware Cloud Foundation

- 9 posts from 8 independent sources in 48 h
- VMware: very widely used in large enterprises
- exploited in the wild (CISA KEV)

CVEs: CVE-2026-41709

Newly exploited in the wild

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

New public exploit code 1

10.0 **CVE-2026-97229** GitLab GitLab METASPLOIT MODULE KEV DETECTION

CVE published Oct 13, 2026

An attacker can execute arbitrary code on the GitLab server without authentication.

New critical CVEs 13

9.8 **CVE-2026-120201** Dromara Jpom EXPLOIT CODE DETECTION
Unauthenticated attackers gain super-administrator access to Jpom 2.10.0 through 2.11.12 by injecting query conditions into the JPOM-USER-TOKEN header.

9.8 **CVE-2026-116512** Wedevs Project Manager – AI Powered Project Management, Task… EXPLOIT CODE
Remote code execution in the Project Manager WordPress plugin through version 4.1.1 via the unsanitized 'id' parameter.

9.1 **CVE-2026-103882** Acadlix Acadlix LMS – AI Quiz Maker, Online Exam & Course Plugin for WordPress
The Acadlix LMS – AI Quiz Maker, Online Exam & Course Plugin for WordPress plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the post_delete_assessment_file_by_id function in all versions up to, and inclu

9.8 **CVE-2026-118235** Wpazleen SimpleForm – Form Maker to Chat Apps with Quiz, Poll and Multi Lead…
An attacker can upload arbitrary files to the server through the handle_upload function in the SimpleForm WordPress plugin, all versions up to and including 3.10.2.

9.8 **CVE-2026-118636** Apache
Untrusted peers sending frames to Apache MINA 3.0's JavaNativeMessageDecoder can gain RCE via gadget chains, as it deserializes without a class filter.

9.8 **CVE-2026-120209** Anji-Plus AJ-Report
Attackers can forge AJ-Report share tokens using a hard-coded JWT secret, then reach unauthenticated remote code execution via the testTransform endpoint.

9.8 **CVE-2026-109220** Addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder
Attacker can inject PHP objects via the customer_note checkout field of the PDF Invoice for WooCommerce WordPress plugin through 7.1.1 due to weak sanitization.

9.8 **CVE-2026-119096** Uncannyowl Uncanny Toolkit for LearnDash
An attacker can bypass authentication in the Uncanny Toolkit for LearnDash WordPress plugin through version 3.8.2 via the email parameter of uo_login_action().

9.8 **CVE-2026-78191**
WebDyne for Perl (2.031 to before 3.022) runs any file with .psp anywhere in its name as a Perl page, letting attackers execute code via such files.

9.1 **CVE-2026-89270** Popupbuilder Popup Builder – Create highly converting, mobile friendly marketing p…
An attacker can bypass authorization in the Popup Builder plugin for WordPress.

9.1 **CVE-2026-116557** Murgroland WP Booking System – Booking Calendar
Authenticated attackers can modify data without proper authorization in WP Booking System – Booking Calendar.

9.8 **CVE-2026-78189**

Attacker can execute .psp files outside the document root via path traversal in the PSGI API route fallback of WebDyne (Perl) versions 3.007 to before 3.022.

9.3 **CVE-2026-117656** Pow-Auth assent

An unauthenticated remote attacker can impersonate another user.

Ransomware 15

15 victims posted to leak sites. Most active: payload (3), vexy (2), interlock (2), emperador (2), whitearmor (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.