Daily brief, Wednesday, November 4, 2026

Nov 3, 7:00 PM to Nov 4, 7:00 PM ET

Generated Nov 6, 2026, 3:54 AM ET

4	1	9	43	74	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 breaking, 3 emerging, 1 newly exploited, 9 with new public exploit code, 43 new critical CVEs, 74 ransomware posts.

Breaking 4

Linux

- 50 posts from 25 independent sources in 48 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- reports of exploitation in the wild
- emergency / unpatched
- official advisory

CVEs: CVE-2026-98432

WordPress Foundation WordPress: Code / command injection

- 12 posts from 11 independent sources in 48 h
- rising: 12 posts in the last 24 h
- Office: widely used in large enterprises
- code / command injection
- exploited in the wild (CISA KEV)
- official advisory

CVEs: CVE-2026-119977

CVE-2026-58115: Auth bypass / access control

- 13 posts from 12 independent sources in 48 h
- Linux kernel: very widely used in large enterprises
- auth bypass / access control
- reports of exploitation in the wild
- official advisory

CVEs: CVE-2026-58115

PHP2Shell · PHP

- 13 posts from 9 independent sources in 48 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- reports of exploitation in the wild

Emerging 3

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

Google Brotli: Memory corruption

- 4 posts from 3 independent sources in 48 h
- Brotli: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code
- official advisory

CVEs: CVE-2026-111497

GitLab: Memory corruption

- 4 posts from 3 independent sources in 48 h
- GitLab / GitHub: 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

Ivanti Connect Secure

- 6 posts from 5 independent sources in 48 h
- rising: 5 posts in the last 24 h
- Ivanti: very widely used in large enterprises
- exploited in the wild (CISA KEV)

CVEs: CVE-2026-118527

Newly exploited in the wild 1

5.5 **CVE-2024-27834** Apple safari CISA KEV
CVE published May 14, 2024
An attacker with arbitrary read and write capability can bypass Pointer Authentication in Apple Safari.

New public exploit code 9

9.4 **CVE-2026-120446** Madong-Code madong-admin-saas NUCLEI TEMPLATE DETECTION
Unauthenticated remote attackers reach tenant management APIs in madong-admin-saas through 5.1.4 (account, bind-plan, sync-data) due to missing auth.

6.5 **CVE-2026-118539** Drupal Commerce Core NUCLEI TEMPLATE DETECTION
Missing Authorization vulnerability in Drupal Commerce Core allows Forceful Browsing. This issue affects Commerce Core versions: from 0.0.0 to 2.41, from 3.0.0 to 3.3.13.

10.0 **CVE-2026-75650** Adobe Commerce and Magento NUCLEI TEMPLATE KEV DETECTION
Known since Sep 8, 2026
Template engine injection in Adobe Commerce and Magento Open Source lets an attacker execute arbitrary code.

8.1 **CVE-2026-109619** PHP Group PHP NUCLEI TEMPLATE KEV DETECTION
CVE published Oct 21, 2026
PHP global state keeps pointers to freed request memory, so later requests read and branch on freed memory (use-after-free) in PHP.

4.3 **CVE-2026-96655** Plex Media Server NUCLEI TEMPLATE KEV DETECTION
Known since Oct 20, 2026
Authenticated Plex Media Server users can force SSRF to arbitrary internal or external addresses via the /video/:/transcode/universal path parameter.

9.9 **CVE-2026-105740** Langflow-Ai langflow NUCLEI TEMPLATE DETECTION
CVE published Oct 5, 2026
An authenticated attacker can execute arbitrary code remotely on Langflow.

9.8 **CVE-2026-54419** NUCLEI TEMPLATE DETECTION
CVE published Jun 18, 2026
claudiopizzillo PIAF-HMS (PBX-In-A-Flash Hotel Management System; no released versions, latest commit 389d2633441b65ced1c104212cd62be2bfca21e5) contains multiple unauthenticated SQL injection vulnerabilities. The application has no authentication mechanism and

9.6 **CVE-2026-88804** SUSE Rancher NUCLEI TEMPLATE DETECTION
CVE published Sep 28, 2026
Unauthenticated remote attackers can inject stored cross-site scripting into the SUSE Rancher UI via public UI settings updates in 2.11 through 2.15.

9.5 **CVE-2026-114509** composer laravel/framework NUCLEI TEMPLATE DETECTION
CVE published Oct 23, 2026
An attacker can bypass authentication and authenticate as an arbitrary existing user in Laravel.

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-2026-116817 (6.5)

New critical CVEs 43

10.0 **CVE-2026-122051** Edimax BR-6208AC EXPLOIT CODE
Remote command injection in Edimax BR-6208AC 1.32 via the /goform/mp endpoint lets an attacker run commands on the device, and a published exploit exists.

9.8 **CVE-2026-122006** Rubyonrails Active Storage EXPLOIT CODE
An attacker gets server read and write operations on Ruby on Rails Active Storage.

10.0 **CVE-2026-121606** Qihoo 360 D621-2
Manipulating the sign argument to verify_sign causes improper firmware signature verification on Qihoo 360 D621-2 and other listed models up to 6.4.9.

10.0 **CVE-2026-121607** Qihoo 360 D603-2
A remote attacker can run OS commands through the host argument of testspeed_command in Qihoo 360 D603-2 and related D600-2, D606-6, and D706 devices up to firmware 6.4.9.

10.0 **CVE-2026-121609** Qihoo 360 Whole Home Router M5
Hard-coded credentials in the boot script of Qihoo 360 Whole Home Router M5 4.0.17.1566 allow remote access to the device; a public exploit is available.

10.0 **CVE-2026-121615** Linksys E5600
A vulnerability was determined in Linksys E5600 1.1.0.26. Affected is an unknown function of the file /cgi-bin/mesh_login.cgi of the component Login Handler. Executing a manipulation can lead to improper authentication. The attack can be launched remotely. The

10.0 **CVE-2026-121932** Linksys E5350
Remote attackers can run OS commands on Linksys E5350 1.0.00.037 via the ping_ip/traceroute_ip parameter of /wizard/apply.cgi; a public exploit exists.

10.0 **CVE-2026-121933** Linksys E5350
Remote attackers can bypass authentication in the Linksys E5350 1.0.00.037 Setup Wizard via the wizard_router_pwd argument to /wizard/apply.cgi, reaching protected settings.

10.0 **CVE-2026-122013** Comfast CF-WR632AX
Path traversal via the filename argument in the multipart parser of /usr/bin/webmgnt on Comfast CF-WR632AX 2.6.0.1 lets an attacker reach files outside the intended directory.

9.9 **CVE-2026-121597** TOTOLINK A950RG
Manipulating the functionType argument of setAppEasyWizardConfig in TOTOLINK A950RG 4.1.2cu.5268_B20221104 triggers a stack-based buffer overflow.

9.9 **CVE-2026-121598** TOTOLINK A950RG
TOTOLINK A950RG 4.1.2cu.5268_B20221104: a manipulated wepkey argument to /cgi-bin/cstecgi.cgi overflows a stack buffer via strcpy, corrupting memory.

9.9 **CVE-2026-121599** TOTOLINK A950RG
TOTOLINK A950RG firmware 4.1.2cu.5268_B20221104 has a stack buffer overflow via wepkey2/wepkey3 in the cstecgi.cgi Multi-SSID handler, allowing memory corruption.

9.9 **CVE-2026-121600** TOTOLINK A950RG
A stack-based buffer overflow in the addEffect argument of setMacFilterRules in the TOTOLINK A950RG MAC Filter Handler lets an attacker corrupt memory.

9.9 **CVE-2026-97693** Xerrors Yuxi
Authenticated low-privileged users of Yuxi 0.6.0.beta1 through 0.7.1 can run commands in Docker sandboxes insufficiently isolated from trusted services.

9.8 **CVE-2026-114549** NoMachine NoMachine
Remote attackers can execute arbitrary code on NoMachine installations without authentication.

9.8 **CVE-2026-92188** Quest Foglight for Databases
Remote attackers can execute arbitrary code on Quest Foglight for Databases installations without authentication.

9.8 **CVE-2026-92190** Quest Foglight for Databases
Remote attackers can execute arbitrary code on Quest Foglight for Databases installations without authentication.

9.8 **CVE-2026-119481** Crocoblock JetFormBuilder
An attacker gets privilege escalation on JetFormBuilder.

9.8 **CVE-2026-65555** Uncanny Owl Uncanny Toolkit for LearnDash
An attacker gets privilege escalation on Uncanny Toolkit for LearnDash.

9.8 **CVE-2026-121952** FreeRDP FreeRDP
An attacker can write data out of bounds on FreeRDP.

23 more critical CVEs in this window: see the dashboard

Ransomware 74

74 victims posted to leak sites. Most active: soul (25), brain cipher (11), safepay (8), play (5), n0n (5).

Financial services hit: Company #132 (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.