Daily brief, Tuesday, November 3, 2026

Nov 2, 7:00 PM to Nov 3, 7:00 PM ET

Generated Nov 6, 2026, 11:03 PM ET

2	1	8	60	27	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 breaking, 3 emerging, 1 newly exploited, 8 with new public exploit code, 60 new critical CVEs, 27 ransomware posts, 1 new breaches.

Breaking 2

PHP2Shell · PHP

- 13 posts from 8 independent sources in 48 h
- rising: 10 posts in the last 24 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-109618

Linux

- 55 posts from 18 independent sources in 48 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- emergency / unpatched
- official advisory

CVEs: CVE-2026-98432

Emerging 3

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

GitLab: Memory corruption

- 6 posts from 4 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

CVE-2026-58115: Auth bypass / access control

- 5 posts from 5 independent sources in 48 h
- rising: 5 posts in the last 24 h
- Linux kernel: very widely used in large enterprises
- auth bypass / access control
- reports of exploitation in the wild

CVEs: CVE-2026-58115

Ivanti Connect Secure: Privilege escalation (2 CVEs)

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

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

Newly exploited in the wild 1

8.1 **CVE-2026-119977** WordPress Foundation WordPress CISA KEV

Attacker gains remote code execution on WordPress Core 4.7 through 7.1.3 via predictable, web-accessible staging paths used during core upgrades.

New public exploit code 8

7.5 **CVE-2026-116690** Mlflow mlflow NUCLEI TEMPLATE DETECTION

Summary On MLflow tracking servers running without authentication, which is the default for mlflow server, a remote attacker can read arbitrary files from the server’s filesystem by creating a model version tagged as a prompt whose source is a schemeless l

10.0 **CVE-2026-97229** GitLab GitLab NUCLEI TEMPLATE KEV DETECTION

CVE published Oct 13, 2026

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

9.3 **CVE-2026-102764** BeyondTrust Remote Support NUCLEI TEMPLATE KEV DETECTION
Known since Oct 16, 2026
A remote attacker bypasses authentication by spoofing and performs file operations on BeyondTrust Remote Support appliances.

9.9 **CVE-2026-7873** IBM Langflow OSS NUCLEI TEMPLATE DETECTION
CVE published Jun 30, 2026
Product not on watchlist.

9.8 **CVE-2026-75128** Chatchat-Space Langchain-Chatchat NUCLEI TEMPLATE DETECTION
CVE published Oct 20, 2026
Unauthenticated remote attackers can execute arbitrary OS commands on Langchain-Chatchat through 0.3.1.3 by calling the POST /tools/call endpoint to invoke the shell tool.

9.8 **CVE-2026-25555** METASPLOIT MODULE DETECTION
CVE published Jun 8, 2026
OpenBullet2 through version 0.3.2 contains an authentication bypass vulnerability in the API key authentication middleware that allows unauthenticated attackers to gain admin access by supplying an empty X-Api-Key header value. Attackers can exploit the middle

9.3 **CVE-2026-112866** WPFactory Product Filter by WBW NUCLEI TEMPLATE DETECTION
CVE published Oct 24, 2026
An attacker performs Blind SQL Injection on WPFactory Product Filter by WBW.

9.1 **CVE-2024-5450** Unknown Bug Library METASPLOIT MODULE
CVE published Jul 13, 2024
Product not on watchlist. Public PoC seen.

4 older CVEs (published more than 7 days earlier) with new exploit code, below the bar (CVSS under 9, not widely used enterprise tech):
CVE-2026-25856 (8.8), CVE-2026-12970 (7.1), CVE-2026-39908 (6.5), CVE-2026-53468 (4.6)

New critical CVEs 60

9.8 **CVE-2026-44267** npm @enspirit/elo EXPLOIT CODE
Unauthenticated attacker can run arbitrary code in Node.js or browser runtime via unfiltered .constructor access in the @enspirit/elo JavaScript emitter.

9.8 **CVE-2026-44266** npm @enspirit/elo
Elo Ruby backend in @enspirit/elo fails to escape '#' in emitted string literals, allowing remote code execution through Ruby interpolation.

9.1 **CVE-2026-109593** SonicWall GMS
An unauthenticated network attacker can read internal files in SonicWall GMS 9.5.2 and earlier, exposing sensitive information.

9.6 **CVE-2026-121156** Google Chrome
Remote attacker executes arbitrary code outside the sandbox in Google Chrome before 157.0.8103.38 via a crafted HTML page, exploiting a Dawn buffer overflow.

9.6 **CVE-2026-121037** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox in Google Chrome on Windows via an out-of-bounds write in ANGLE, using a crafted HTML page.

9.6 **CVE-2026-121247** Google Chrome
Remote attacker gets arbitrary code execution outside the sandbox in Google Chrome for Android before 157.0.8103.38 via a crafted HTML page.

9.6 **CVE-2026-121086** Google Chrome
Buffer overflow in Skia in Google Chrome before 157.0.8103.38 lets a remote attacker run arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-121249** Google Chrome
Buffer overflow in ANGLE in Google Chrome before 157.0.8103.38 lets a remote attacker execute arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-121035** Google Chrome
A use-after-free in Prerender in Google Chrome before 157.0.8103.38 lets a remote attacker run arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-120931** Google Chrome
Remote attacker can execute arbitrary code outside the sandbox in Google Chrome on Android via an out-of-bounds write in WebGL, using a crafted HTML page.

9.6 **CVE-2026-121229** Google Chrome
Memory corruption in ANGLE in Google Chrome on Android before 157.0.8103.38 lets a remote attacker run arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-121246** Google Chrome
Use-after-free in WebGL in Chrome for Android before 157.0.8103.38 lets a remote attacker run arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-121126** Google Chrome
Use after free in Chrome before 157.0.8103.38 lets a remote attacker execute arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-121074** Google Chrome
Memory corruption in Google Chrome GPU on Android before 157.0.8103.38 lets a remote attacker run arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-121185** Google Chrome
Remote code execution outside the Chrome sandbox via a crafted HTML page, requiring social engineering to lure the user, in Google Chrome before 157.0.8103.38.

9.6 **CVE-2026-121089** Google Chrome
Remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page exploiting a use-after-free in WebGPU in Chrome before 157.0.8103.38.

9.6 **CVE-2026-121114** Google Chrome
Remote attacker executes arbitrary code outside the sandbox in Google Chrome before 157.0.8103.38 via a crafted HTML page, exploiting a TabStrip use-after-free.

9.6 **CVE-2026-121148** Google Chrome
Use-after-free in ANGLE in Google Chrome before 157.0.8103.38 lets a remote attacker run arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-121189** Google Chrome
Use-after-free in Google Chrome before 157.0.8103.38 lets a remote attacker execute arbitrary code outside the sandbox via a crafted HTML page.

9.6 **CVE-2026-121214** Google Chrome
Remote attacker executes arbitrary code outside the sandbox via a crafted HTML page in Google Chrome before 157.0.8103.38 (use-after-free in Passwords).

40 more critical CVEs in this window: see the dashboard

Ransomware 27

27 victims posted to leak sites. Most active: n0n (10), booba team (4), akira (3), whitearmor (1), the gentlemen (1).

New data breaches 1

Harvard harvard.edu 850,537 accounts

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.