Daily brief, Saturday, November 7, 2026

Nov 6, 7:00 PM to Nov 7, 7:00 PM ET

Generated Nov 8, 2026, 9:23 PM ET

5	0	0	67	44	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 breaking, 1 emerging, 67 new critical CVEs, 44 ransomware posts.

Breaking 5

SonicWall SonicOS

- 18 posts from 16 independent sources in 48 h
- rising: 18 posts in the last 24 h
- SonicWall: widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- official advisory

CVEs: CVE-2026-19868

OpenBSD OpenSSH: Auth bypass / access control

- 18 posts from 14 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

Linux

- 19 posts from 11 independent sources in 48 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code
- Cloudflare Zero Wire: needs attention

CVEs: CVE-2026-98432

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

Apple safari: Auth bypass / access control

- 8 posts from 7 independent sources in 48 h
- macOS / iOS: very widely used in large enterprises
- auth bypass / access control
- exploited in the wild (CISA KEV)
- named threat actor activity

CVEs: CVE-2024-27834

Emerging 1

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

PHP Group PHP: Memory corruption (2 CVEs)

- 3 posts from 3 independent sources in 48 h
- PHP: very widely used in large enterprises
- exploited in the wild (CISA KEV)
- public exploit code
- Cloudflare Zero Wire: needs attention

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

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.

New critical CVEs 67

9.1 **CVE-2026-118066** Latepoint Appointment Booking Plugin – LatePoint | Calendar & Scheduling for W…
Authentication bypass in the LatePoint appointment booking plugin for WordPress, through version 5.7.6, lets attackers take over user accounts.

10.0 **CVE-2026-123966** Tenda AC19
Heap buffer overflow via the deviceId argument of /goform/saveParentControlInfo in Tenda AC19 16.03.10.07 lets remote attackers corrupt memory.

9.9 **CVE-2026-16920** IBM API Connect
A remote authenticated attacker can bypass security restrictions in IBM API Connect 12.1.0.0 through 12.1.1.2 via a confused deputy flaw.

9.9 **CVE-2026-16884** IBM API Connect
A remote attacker can obtain sensitive information from IBM API Connect 12.1.0.0 through 12.1.1.2 via XML external entity (XXE) injection.

9.9 **CVE-2026-17049** IBM API Connect
+2 more CVEs in the same release
A remote authenticated attacker can read sensitive information and modify arbitrary documents in IBM API Connect 12.1.0.0 through 12.1.1.2 via an authorization bypass using user-controlled keys.

9.9 **CVE-2026-17117** IBM API Connect
+16 more CVEs in the same release
Authenticated remote attacker runs arbitrary code in IBM API Connect 10.0.8.0-10.0.8.12 and 12.1.0.0-12.1.1.2 by setting system-only object attributes.

9.9 **CVE-2026-17132** IBM API Connect
+2 more CVEs in the same release
A remote authenticated attacker can execute arbitrary SQL commands in IBM API Connect 12.1.0.0 through 12.1.1.2 via improper neutralization of SQL special elements.

9.9 **CVE-2026-17239** IBM API Connect
A remote authenticated attacker can execute arbitrary code in IBM API Connect 12.1.0.0 through 12.1.1.2 via a path traversal flaw.

9.9 **CVE-2026-17354** IBM API Connect
A remote authenticated attacker can perform arbitrary file writes via path traversal in IBM API Connect versions 12.1.0.0 through 12.1.1.2.

9.9 **CVE-2026-123957** TOTOLINK CA300-PoE
Remote attackers can trigger a buffer overflow via the ipStart argument of setIpQosRules in /cgi-bin/cstecgi.cgi on TOTOLINK CA300-PoE 6.2c.884.

9.9 **CVE-2026-123958** TOTOLINK CA300-PoE
Remote attacker triggers a buffer overflow in TOTOLINK CA300-PoE 6.2c.884 via lanDns, lanSecDns, or langType in setLanConfig; public exploit exists.

9.9 **CVE-2026-123960** TOTOLINK CA300-PoE
Remote attacker can overflow a buffer in TOTOLINK CA300-PoE 6.2c.884 via pppoeUser, priDns, or secDns in setWanConfig (cstecgi.cgi); public exploit exists.

9.9 **CVE-2026-123961** TOTOLINK CA300-PoE
Remote attacker can trigger a buffer overflow via KeyStr in setWiFiBasicConfig of TOTOLINK CA300-PoE 6.2c.884 /cgi-bin/cstecgi.cgi; a public exploit is disclosed.

9.8 **CVE-2026-93754** Envoyproxy Gateway
Attacker gets remote code execution via arbitrary file upload in payever WooCommerce Gateway WordPress plugin through 4.8.0.

9.8 **CVE-2026-123218** IBM Aspera Faspex
An authorized IBM Aspera Faspex 5.0.0 through 5.0.19 user can craft a specific message to bypass authorization and gain full administrative privileges.

9.8 **CVE-2026-17362** IBM API Connect V12 OnPrem
Lets a remote attacker create, modify, or delete tenants in IBM API Connect V12 OnPrem 12.1.0.0 through 12.1.1.2 because authorization checks are missing.

9.8 **CVE-2026-19803** Printcart Printcart Store – Web to Print Product Designer for WooCommerce
Attacker can upload arbitrary files to the Printcart Store WooCommerce plugin for WordPress through 2.13.2 via the nbu_crop_image AJAX url parameter.

9.8 **CVE-2026-16720** IBM API Connect
Remote attacker can obtain valid access tokens for other users in IBM API Connect 10.0.8.0–10.0.8.12 and 12.1.0.0–12.1.1.2 due to improper authentication.

9.8 **CVE-2026-17278** IBM API Connect
A remote attacker gains unauthorized access to API catalog and runtime configuration data in IBM API Connect 12.1.0.0 through 12.1.1.2 via improper authentication.

9.8 **CVE-2026-17301** IBM API Connect
Unauthenticated attackers can bypass authentication in IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 due to improper cryptographic signature verification.

27 more critical CVEs in this window: see the dashboard

Ransomware 44

44 victims posted to leak sites. Most active: n0n (14), qilin (10), metaencryptor (7), payload (4), nightspire (3).

Financial services hit: Company #140 (n0n), Company #138 (n0n), AXE - EXPERTS (qilin), Higginbotham (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.