Daily brief, Monday, November 2, 2026

Nov 1, 7:00 PM to Nov 2, 7:00 PM ET

Generated Nov 6, 2026, 3:24 PM ET

3	0	2	37	51	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 breaking, 2 with new public exploit code, 37 new critical CVEs, 51 ransomware posts.

Breaking 3

Linux (2 CVEs)

- 106 posts from 15 independent sources in 48 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code
- emergency / unpatched
- official advisory

CVEs: CVE-2026-98432, CVE-2026-9843

PHP2Shell · PHP

- 10 posts from 8 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

CVEs: CVE-2026-46300

Ivanti Connect Secure: Privilege escalation (2 CVEs)

- 7 posts from 6 independent sources in 48 h
- rising: 5 posts in the last 24 h
- Ivanti: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)

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

Newly exploited in the wild

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

New public exploit code 2

9.5 **CVE-2026-116366** ClickHouse ClickHouse NUCLEI TEMPLATE DETECTION
An attacker can execute arbitrary code on the ClickHouse Server without authentication.

4.3 **CVE-2026-96652** Plex Media Server NUCLEI TEMPLATE KEV DETECTION
Known since Oct 20, 2026
An attacker with any X-Plex-Token value can force Plex Media Server to send POST requests to an arbitrary destination via the 'protocol' parameter (SSRF).

New critical CVEs 37

9.8 **CVE-2026-86596** Clavaque s2Member – Excellent for All Kinds of Memberships, Cont… EXPLOIT CODE
Remote code execution in the s2Member WordPress plugin (versions up to and including 260927) via the item_name parameter, due to insufficient sanitization.

9.8 **CVE-2026-58868** Google Android EXPLOIT CODE
Remote code execution in Google Android via a heap out-of-bounds write in FrameDecoder.cpp, requiring no extra privileges or user interaction.

9.4 **CVE-2026-120446** Madong-Code madong-admin-saas EXPLOIT CODE 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.

9.8 **CVE-2026-120442** Xianhc ape-volo-admin EXPLOIT CODE DETECTION
Unauthenticated attackers forge admin JWTs with a hardcoded signing key in appsettings.json, gaining full admin access to ape-volo-admin before 3.6.1.

9.8 **CVE-2026-58876** Google Android
Use-after-free memory corruption in multiple Android locations lets a remote attacker execute code with no added privileges and no user interaction.

9.8 **CVE-2026-58936** Google Android
A use-after-free in png_set_tRNS in Google Android's pngset.c allows remote code execution with no extra execution privileges and no user interaction.

9.8 **CVE-2026-58968** Google Android
Remote attacker gains privilege escalation via a double free memory corruption in Android's oapvd_vlc_metadata (oapv_vlc.c), with no user interaction required.

10.0 **CVE-2026-120276** WAVLINK WN536AX6-A

Attacker runs OS commands on WAVLINK WN536AX6-A V260507_2.0.0 via command injection in the group_name argument of the web management interface.

10.0 **CVE-2026-120277** WAVLINK

Attacker can inject OS commands via the group_name argument in the WireGuard CLI group handler of WAVLINK WN536AX6-A V260507_2.0.0, running commands on the device.

10.0 **CVE-2026-120345** WAVLINK

A remote attacker can inject OS commands via the data argument of the DNS Resolution Handler in WAVLINK WN551X3-A firmware M51X3_V251020-WO-182e965.

10.0 **CVE-2026-120279** WAVLINK WN536AX6-A

Remote attacker can inject OS commands through the file_id argument in WAVLINK WN536AX6-A V260507's /protocol.csp, gaining command execution on the device.

10.0 **CVE-2026-120280** WAVLINK WN536AX6-A

An attacker can inject OS commands via the group_id and group_name arguments in the WireGuard handler of WAVLINK WN536AX6-A V260507 firmware, initiated remotely.

10.0 **CVE-2026-120344** WAVLINK WN551X3-A

A remote attacker can run OS commands on WAVLINK WN551X3-A firmware M51X3_V251020 by injecting input into the group_name argument of the WireGuard CLI Group Handler.

9.9 **CVE-2026-120282** WAVLINK WN536AX6-A

Remote attacker can inject OS commands via the mac argument of host_black in /protocol.csp on WAVLINK WN536AX6-A V260507, gaining command execution.

9.3 **CVE-2026-116606** Barracuda Networks Barracuda Email Security Gateway (ESG)

Unauthenticated remote attacker bypasses auth in Barracuda Email Security Gateway before 9.4.0.030 and imports a crafted backup, modifying global configuration.

9.1 **CVE-2026-120213** @Fastify/Http-Proxy @fastify/http-proxy

Path traversal in @fastify/http-proxy 9.0.0-11.6.5 lets clients reach upstream paths outside the pinned prefix via URL-decoded route parameters when parameterized prefix and rewritePrefix are used.

9.9 **CVE-2026-120322** Termix-SSH Termix

Termix up to 2.9.2 has a path traversal via the destPath argument of /plugin-api/file-manager/transferToHost, letting remote attackers reach files outside intended directories.

9.8 **CVE-2026-102435** Themefic Ultra Addons for Contact Form 7

The Ultra Addons for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the _getObjAttr function in all versions up to, and including, 3.5.54. This makes it possible for unauthenticated atta

10.0 **CVE-2026-120283** Linksys

Remote attacker overflows a stack buffer in Linksys E8450 1.2.00.360516 via a crafted hidden_timezone argument to portal.cgi, where strcpy is used unsafely.

10.0 **CVE-2026-120281** Wavlink

Remote attacker can trigger a stack-based buffer overflow in the OpenVPN Handler of Wavlink WN536AX6-A V260507 via the openvpn_ip argument in /protocol.csp.

17 more critical CVEs in this window: see the dashboard

Ransomware 51

51 victims posted to leak sites. Most active: the gentlemen (24), n0n (5), orova (4), akira (3), ransomhouse (2).

Financial services hit: Isapre Consalud (qilin), Company #117 (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.