Daily brief, Sunday, November 1, 2026

Oct 31, 8:00 PM to Nov 1, 7:00 PM ET

Generated Nov 6, 2026, 11:01 PM ET

5	0	0	24	16	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 breaking, 2 emerging, 24 new critical CVEs, 16 ransomware posts.

Breaking 5

PHP2Shell · PHP

- 32 posts from 21 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-2026-46300, CVE-2026-109618

Linux (2 CVEs)

- 107 posts from 24 independent sources in 48 h
- rising: 83 posts in the last 24 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code
- official advisory

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

Node2Shell · Node.js

- 6 posts from 6 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

GitLab: Memory corruption

- 8 posts from 6 independent sources in 48 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-97229

Ivanti Connect Secure: Privilege escalation (2 CVEs)

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

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

Emerging 2

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

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

- 3 posts from 3 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

Cisco Secure Firewall ASA Software and Cisco Secure FTD Software

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

CVEs: CVE-2026-76418

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 24

9.1 **CVE-2026-120229** WAVLINK WN553X1-B
An attacker can inject OS commands remotely on WAVLINK WN553X1-B.

9.9 **CVE-2026-120227** WAVLINK WN701AE
A remote attacker can inject OS commands through the rule_name argument of the static route deletion function in WAVLINK WN701AE M01AE_V260105 web backend.

9.9 **CVE-2026-120230** WAVLINK WN701AE
Remote attacker can inject OS commands via the vlan_name argument of del_vlan_group in WAVLINK WN701AE (260105) web backend, and a public exploit exists.

10.0 **CVE-2026-120195** WAVLINK WL-WN579A3-A
An attacker can inject OS commands via the wlan_ssid argument in the Initial Setup Wizard of WAVLINK WL-WN579A3-A firmware, gaining command execution on the device.

10.0 **CVE-2026-120198** WAVLINK WL-WN530BE1-A
A remote attacker can inject OS commands via the group_name and IP-FROM arguments of /protocol.csp in WAVLINK WL-WN530BE1-A V251117.

9.9 **CVE-2026-120196** WAVLINK WN579X3-D
Remote attackers can inject OS commands via the Name argument of the port_forward function in /cgi-bin/wapi.cgi on WAVLINK WN579X3-D V250402.

9.9 **CVE-2026-120197** WAVLINK WL-WN530HG4B
Remote OS command injection in WAVLINK WL-WN530HG4B (M_V260724) lets attackers run commands via the Name argument of port_forward in /cgi-bin/wapi.cgi.

9.9 **CVE-2026-120231** WAVLINK WN553X1-B
A remote attacker can inject OS commands through the file_id argument in the OpenVPN CLI handler of WAVLINK WN553X1-B V260403_2.0.0.

9.9 **CVE-2026-120240** WAVLINK WN553X1-B
Attacker can inject OS commands via the group_id or group_name argument in the WireGuard CLI Group Handler of WAVLINK WN553X1-B firmware V260403_2.0.0.

9.9 **CVE-2026-120239** WAVLINK WN553X1-B
An attacker can inject OS commands through the file_id argument in the WireGuard CLI handler of WAVLINK WN553X1-B V260403_2.0.0.

9.9 **CVE-2026-120238** WAVLINK WN553X1-B
Remote attackers can run OS commands via file_id in the ovpn_file handler of WAVLINK WN553X1-B 260403_2.0.0; a public exploit exists.

9.9 **CVE-2026-120228** WAVLINK WN553X1-B
Remote OS command injection via the group_id/group_name argument of WAVLINK WN553X1-B V260403_2.0.0's ioos service lets attackers run arbitrary commands.

10.0 **CVE-2026-120189** D-Link
A remote attacker can trigger a stack-based buffer overflow in the TFTP upload filename handler of D-Link DIR-505 firmware 1.10B02.

10.0 **CVE-2026-120338** PrefectHQ prefab-ui
Attacker-supplied Python run by prefab-ui 0.14.0 through 0.20.2's Generative UI sandbox escapes isolation because the Deno launcher starts with unrestricted permissions.

9.1 **CVE-2026-120225** Oray Pugongying X5 Pro
An attacker can traverse files and directories remotely on Oray Pugongying X5 Pro.

9.9 **CVE-2026-120308** Beam-Cloud Beta9 gateway
An authenticated Beta9 gateway tenant can attach volumes not owned by its workspace when deploying a function, endpoint, or task queue, because the volume identifier is not validated.

9.9 **CVE-2026-120307** Beam-Cloud Beta9 worker
Path traversal in the Beta9 worker's sandbox file API lets a tenant's container path resolve to worker host files outside the container's mounts.

9.9 **CVE-2026-120224** Oray Pugongying X5 Pro
Remote privilege escalation via improper authorization in the API Authorization component of Oray Pugongying X5 Pro up to 7.6.1; public exploit released.

9.9 **CVE-2026-120306** Beam-Cloud Beta9 worker
Beta9 worker's Buildah runs tenant image-build commands in chroot isolation, so a tenant escalates privileges by keeping the worker pod's access.

9.3 **CVE-2026-62048** Liquid Web / StellarWP BookIt
An attacker gets SQL injection on Liquid Web / StellarWP BookIt with no authentication required.

4 more critical CVEs in this window: see the dashboard

Ransomware 16

16 victims posted to leak sites. Most active: qilin (10), interlock (2), shiba (1), lockbit5 (1), hyflock (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.