Daily brief, Thursday, November 5, 2026

Nov 4, 7:00 PM to Nov 5, 7:00 PM ET

Generated Nov 6, 2026, 9:20 AM ET

5	0	1	39	22	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 breaking, 2 emerging, 1 with new public exploit code, 39 new critical CVEs, 22 ransomware posts.

Breaking 5

Linux

- 27 posts from 17 independent sources in 48 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- reports of exploitation in the wild
- Cloudflare Zero Wire: needs attention

CVEs: CVE-2026-98432

WordPress Foundation WordPress: Code / command injection

- 17 posts from 15 independent sources in 48 h
- Office: widely used in large enterprises
- code / command injection
- exploited in the wild (CISA KEV)
- public exploit code
- official advisory

CVEs: CVE-2026-119977

CVE-2026-58115: Auth bypass / access control

- 11 posts from 11 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

Debian

- 10 posts from 9 independent sources in 48 h
- rising: 10 posts in the last 24 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- named threat actor activity
- official advisory

CVEs: CVE-2026-109518

Apple safari: Auth bypass / access control

- 7 posts from 6 independent sources in 48 h
- rising: 7 posts in the last 24 h
- macOS / iOS: very widely used in large enterprises
- auth bypass / access control
- exploited in the wild (CISA KEV)

CVEs: CVE-2024-27834

Emerging 2

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

Ivanti Connect Secure

- 5 posts from 4 independent sources in 48 h
- Ivanti: very widely used in large enterprises
- exploited in the wild (CISA KEV)

CVEs: CVE-2026-118527

SonicWall GMS: Information disclosure (2 CVEs)

- 5 posts from 5 independent sources in 48 h
- SonicWall: widely used in large enterprises
- remote code execution / auth bypass

CVEs: CVE-2026-109593, CVE-2026-109594

Newly exploited in the wild

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

New public exploit code 1

9.8 **CVE-2026-120201** Dromara Jpom NUCLEI TEMPLATE DETECTION

An attacker gains super-administrator access in Jpom by injecting malicious query conditions into the JPOM-USER-TOKEN header.

New critical CVEs 39

9.8 **CVE-2026-116779** FreeSWITCH FreeSWITCH EXPLOIT CODE

+2 more CVEs in the same release

FreeSWITCH before 1.11.3 has a command injection flaw where an attacker can inject commands through the To user of an inbound SIP MESSAGE.

10.0 **CVE-2026-73117** Apache Apache Juneau

Apache Juneau REST server passes unchecked header and redirect values, enabling HTTP response splitting via CRLF injection when apps use user input.

10.0 **CVE-2026-121489** Apache Apache Juneau

Apache Juneau's DirectoryResource lets an attacker read, upload or delete files outside its root directory when those settings are enabled.

10.0 **CVE-2026-96677** Apache Apache Juneau

Apache Juneau HTML document serialization fails to HTML-encode variable substitutions in page chrome fields, allowing cross-site scripting in generated pages.

10.0 **CVE-2026-73099** Apache Apache Juneau

Apache Juneau REST server CSRF: a cross-site link forges endpoint requests with an attacker-chosen body via the default-enabled 'content' query parameter.

10.0 **CVE-2026-73100** Apache Apache Juneau

Apache Juneau's default REST logger logs unredacted Authorization and Cookie headers for server-error requests, exposing them to any client able to trigger one.

10.0 **CVE-2026-73101** Apache Apache Juneau

Attackers can read internal exception classes and messages from Apache Juneau REST server error responses, via the Thrown header and error bodies.

10.0 **CVE-2026-73098** Apache Apache Juneau

Apache Juneau initializes any classpath class named in input parsed into a java.lang.Class property, letting an attacker run its static initializers.

10.0 **CVE-2026-73116** Apache Apache Juneau

Apache Juneau RestClient keeps credential headers when following redirects to another host, port, or HTTP, exposing those credentials to the redirect target server.

9.9 **CVE-2026-122313** Kyverno Kyverno
Namespace-scoped tenants of Kyverno 1.17.0 before 1.19.2 can modify resources in other namespaces via unchecked NamespacedMutatingPolicy target CEL expressions.

9.9 **CVE-2026-122303** Kyverno kyverno
An authorization bypass in Kyverno 1.17.0 before 1.19.2 lets namespace tenants overwrite resources in other namespaces via NamespacedMutatingPolicy mutate-existing target expressions.

9.9 **CVE-2026-122304** Kyverno kyverno
Namespace admins in Kyverno 1.17.0 before 1.19.2 can escape namespace confinement through the cleanup controller, bypassing authorization checks.

9.9 **CVE-2026-122310** Kyverno kyverno
Kyverno 1.19.1 before 1.19.2 lets a namespace-scoped user who can create a Policy hide ../ path segments behind # or ? to reach cluster-scoped API endpoints.

9.9 **CVE-2026-122311** Kyverno kyverno
Kyverno 1.16.0-1.19.1 path traversal lets a tenant allowed to create NamespacedValidatingPolicy read and write cluster resources outside its namespace.

9.9 **CVE-2026-71550** SuiteCRM SuiteCRM
+1 more CVEs in the same release
Path traversal in SuiteCRM's workflow controller aow_action value lets attackers include files outside the intended path via require_once() in versions before 7.15.2 and 8.10.2.

9.9 **CVE-2026-111489** TPC Software Matchpoint
A static credential embedded in TPC Software's MatchPoint mobile app returns an 'autorizado' token granting unauthenticated access to API services.

9.9 **CVE-2026-111490** TPC Software Matchpoint
Attacker accesses personal, banking, and financial data of other users in TPC Software Matchpoint API by manipulating the actingasuser header.

9.8 **CVE-2026-122302** Kyverno kyverno
An attacker can create resources beyond their RBAC permissions using Kyverno.

9.8 **CVE-2026-19256** Unknown All In One Login
An unauthenticated attacker can brute-force the short numeric passwordless email login code to sign in via the All In One Login WordPress plugin before 2.5.0.

9.8 **CVE-2026-100109** Unknown Security For WooCommerce
Unauthenticated attackers can create administrator accounts in the Security For WooCommerce WordPress plugin 1.0.10-1.0.16 by setting the new user's role.

16 more critical CVEs in this window: see the dashboard

Ransomware 22

22 victims posted to leak sites. Most active: n0n (7), akira (4), qilin (2), leakeddata (2), redact (1).

Financial services hit: Insurance Audit Services (qilin), Delta Dental of Missouri (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.