Daily brief, Sunday, March 29, 2026

Mar 28, 8:00 PM to Mar 29, 8:00 PM ET

Generated Nov 7, 2026, 10:17 AM ET

0	0	0	8	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

8 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

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

8

9.8 **CVE-2026-0558** Lollms lollms DETECTION

A vulnerability in parisneo/lollms, up to and including version 2.2.0, allows unauthenticated users to upload and process files through the `/api/files/extract-text` endpoint. This endpoint does not enforce authentication, unlike other file-related endpoints,

9.8 **CVE-2026-4176** Perl perl

Perl versions from 5.9.4 before 5.40.4-RC1, from 5.41.0 before 5.42.2-RC1, from 5.43.0 before 5.43.9 contain a vulnerable version of Compress::Raw::Zlib. Compress::Raw::Zlib is included in the Perl package as a dual-life core module, and is vulnerable to CVE-2

9.9 **CVE-2026-32922** Openclaw openclaw

OpenClaw before 2026.3.11 contains a privilege escalation vulnerability in device.token.rotate that allows callers with operator.pairing scope to mint tokens with broader scopes by failing to constrain newly minted scopes to the caller's current scope set. Att

9.8 **CVE-2026-4851** Casiano grid\

GRID::Machine versions through 0.127 for Perl allows arbitrary code execution via unsafe deserialization. GRID::Machine provides Remote Procedure Calls (RPC) over SSH for Perl. The client connects to remote hosts to execute code on them. A compromised or malic

9.8 **CVE-2026-32973** Openclaw openclaw

OpenClaw before 2026.3.11 contains an exec allowlist bypass vulnerability where matchesExecAllowlistPattern improperly normalizes patterns with lowercasing and glob matching that overmatches on POSIX paths. Attackers can exploit the ? wildcard matching across

9.8 **CVE-2026-32987** Openclaw openclaw

OpenClaw before 2026.3.13 allows bootstrap setup codes to be replayed during device pairing verification in src/infra/device-bootstrap.ts. Attackers can verify a valid bootstrap code multiple times before approval to escalate pending pairing scopes, including

9.8 **CVE-2026-32975** Openclaw openclaw

OpenClaw before 2026.3.12 contains a weak authorization vulnerability in Zalouser allowlist mode that matches mutable group display names instead of stable group identifiers. Attackers can create groups with identical names to allowlisted groups to bypass chan

9.8 **CVE-2026-32924** Openclaw openclaw

OpenClaw before 2026.3.12 contains an authorization bypass vulnerability where Feishu reaction events with omitted chat_type are misclassified as p2p conversations instead of group chats. Attackers can exploit this misclassification to bypass groupAllowFrom an

Ransomware

No leak-site posts collected.

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.