Daily brief, Saturday, March 7, 2026

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

Generated Nov 7, 2026, 2:12 PM ET

0	0	0	9	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

9 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

9

9.8 **CVE-2026-30824** Flowiseai flowise DETECTION

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.0.13, the NVIDIA NIM router (/api/v1/nvidia-nim/*) is whitelisted in the global authentication middleware, allowing unauthenticated access to privileged

9.8 **CVE-2026-30821** Flowiseai flowise

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.0.13, the /api/v1/attachments/:chatflowId/:chatId endpoint is listed in WHITELIST_URLS, allowing unauthenticated access to the file upload API. While th

9.8 **CVE-2026-25070** Seekswan zikestor sks8310-8x firmware

XikeStor SKS8310-8X Network Switch firmware versions 1.04.B07 and prior contain an OS command injection vulnerability in the /goform/PingTestSet endpoint that allows unauthenticated remote attackers to execute arbitrary operating system commands. Attackers can

9.9 **CVE-2026-30861** Tencent weknora

WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. From version 0.2.5 to before version 0.2.10, an unauthenticated remote code execution (RCE) vulnerability exists in the MCP stdio configuration validation. The

9.9 **CVE-2026-30860** Tencent weknora

WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.12, a remote code execution (RCE) vulnerability exists in the application's database query functionality. The validation system fails to r

9.8 **CVE-2026-30863** Parseplatform parse-server

Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.10 and 9.5.0-alpha.11, the Google, Apple, and Facebook authentication adapters use JWT verification to validate identity tokens. When

9.8 **CVE-2026-25072** Seekswan zikestor sks8310-8x firmware

XikeStor SKS8310-8X Network Switch firmware versions 1.04.B07 and prior contain a predictable session identifier vulnerability in the /goform/SetLogin endpoint that allows remote attackers to hijack authenticated sessions. Attackers can predict session identif

9.3 **CVE-2026-29191** Zitadel zitadel

ZITADEL is an open source identity management platform. From version 4.0.0 to 4.11.1, a vulnerability in Zitadel's login V2 interface was discovered that allowed a possible account takeover via XSS in /saml-post Endpoint. This issue has been patched in version

9.1 **CVE-2026-30832** Charm soft serve

Soft Serve is a self-hostable Git server for the command line. From version 0.6.0 to before version 0.11.4, an authenticated SSH user can force the server to make HTTP requests to internal/private IP addresses by running repo import with a crafted --lfs-endpoi

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.