Daily brief, Monday, April 6, 2026

Apr 5, 8:00 PM to Apr 6, 8:00 PM ET

Generated Nov 7, 2026, 8:45 AM ET

0	1	0	27	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 27 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.1 **CVE-2026-35616** Fortinet FortiClient EMS CISA KEV DETECTION

Improper access control in Fortinet FortiClient EMS lets an attacker gain unauthorized access to sensitive data and perform arbitrary actions.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

27

9.1 **CVE-2026-35616** Fortinet FortiClient EMS KEV EXPLOIT CODE DETECTION

Improper access control in Fortinet FortiClient EMS lets an attacker gain unauthorized access to sensitive data and perform arbitrary actions.

9.1 **CVE-2026-26026** Glpi-Project glpi EXPLOIT CODE

GLPI is a free asset and IT management software package. From 11.0.0 to before 11.0.6, template injection by an administrator lead to RCE. This vulnerability is fixed in 11.0.6.

9.8 **CVE-2026-35171** Linuxfoundation kedro

Kedro is a toolbox for production-ready data science. Prior to 1.3.0, Kedro allows the logging configuration file path to be set via the KEDRO_LOGGING_CONFIG environment variable and loads it without validation. The logging configuration schema supports the sp

9.8 **CVE-2026-31405** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: media: dvb-net: fix OOB access in ULE extension header tables The ule_mandatory_ext_handlers[] and ule_optional_ext_handlers[] tables in handle_one_ule_extension() are declared with 255 elemen

10.0 **CVE-2026-34976** Dgraph dgraph DETECTION

Dgraph is an open source distributed GraphQL database. Prior to 25.3.1, the restoreTenant admin mutation is missing from the authorization middleware config (admin.go), making it completely unauthenticated. Unlike the similar restore mutation which requires Gu

9.8 **CVE-2026-31059** Utt 520w firmware

A remote command execution (RCE) vulnerability in the /goform/formDia component of UTT Aggressive HiPER 520W v3v1.7.7-180627 allows attackers to execute arbitrary commands via a crafted string.

9.8 **CVE-2026-34977** Aperisolve aperisolve

Aperi'Solve is an open-source steganalysis web platform. In versions 3.1.3 through 3.2.0, when uploading a JPEG, a user can specify an optional password to accompany the JPEG. This password is then directly passed into an expect command, which is then subseque

9.8 **CVE-2026-35392** Goshs goshs

goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.3, PUT upload in httpserver/updown.go has no path sanitization. This vulnerability is fixed in 2.0.0-beta.3.

9.8 **CVE-2026-35393** Goshs goshs

goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.3, the POST multipart upload directory not sanitized. This vulnerability is fixed in 2.0.0-beta.3.

9.8 **CVE-2026-35471** Goshs goshs

goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.3, tdeleteFile() missing return after path traversal check. This vulnerability is fixed in 2.0.0-beta.3.

9.8 **CVE-2026-35052** Man d-tale

D-Tale is the combination of a Flask back-end and a React front-end to view & analyze Pandas data structures. Prior to 3.22.0, users hosting D-Tale publicly while using a redis or shelf storage layer could be vulnerable to remote code execution allowing attack

10.0 **CVE-2026-34444** Scoder lupa

Lupa integrates the runtimes of Lua or LuaJIT2 into CPython. In 2.6 and earlier, attribute_filter is not consistently applied when attributes are accessed through built-in functions like getattr and setattr. This allows an attacker to bypass the intended restr

9.1 **CVE-2026-35030** Litellm litellm

LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.83.0, when JWT authentication is enabled (enable_jwt_auth: true), the OIDC userinfo cache uses token[:20] as the cache key. JWT headers produced by the same signin

10.0 **CVE-2026-34208** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Prior to 0.8.36, SandboxJS blocks direct assignment to global objects (for example Math.random = ...), but this protection can be bypassed through an exposed callable constructor path: this.constructor.call(target,

9.1 **CVE-2026-35174** Chyrplite chyrp lite

Chyrp Lite is an ultra-lightweight blogging engine. Prior to 2026.01, a path traversal vulnerability exists in the administration console that allows an administrator or a user with Change Settings permission to change the uploads path to any folder. This vuln

9.8 **CVE-2026-35047** Ajax30 bravecms

Brave CMS is an open-source CMS. Prior to 2.0.6, an Unrestricted File Upload vulnerability in the CKEditor endpoint allows attackers to upload arbitrary files, including executable scripts. This may lead to Remote Code Execution (RCE) on the server, potentiall

10.0 **CVE-2025-54328** Samsung exynos 980 firmware

An issue was discovered in SMS in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. A Stack-based Buffer Ov

9.8 **CVE-2026-35178** Forceworkbench forceworkbench

Workbench is a suite of tools for administrators and developers to interact with Salesforce.com organizations via the Force.com APIs. Prior to 65.0.0, Workbench contains remote code execution vulnerability in the timezone conversion flow, which processes attac

9.1 **CVE-2026-35050** Oobabooga textgen

text-generation-webui is an open-source web interface for running Large Language Models. Prior to 4.1.1, users can save extention settings in "py" format and in the app root directory. This allows to overwrite python files, for instance the "download-model.py"

9.8 **CVE-2026-31151** Kaleris yard management solutions

An issue in the login mechanism of Kaleris YMS v7.2.2.1 allows attackers to bypass login verification to access the application 's resources.

7 more critical CVEs in this window: see the dashboard

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.