Daily brief, Thursday, April 23, 2026

Apr 22, 8:00 PM to Apr 23, 8:00 PM ET

Generated Nov 7, 2026, 5:41 AM ET

0	1	0	45	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 45 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 1

9.3 **CVE-2026-39987** Marimo Marimo CISA KEV DETECTION

Unauthenticated attackers can execute arbitrary system commands and gain shell access on Marimo through a pre-authorization remote code execution flaw.

New public exploit code

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

New critical CVEs 45

9.3 **CVE-2026-39987** Marimo Marimo KEV EXPLOIT CODE DETECTION

Unauthenticated attackers can execute arbitrary system commands and gain shell access on Marimo through a pre-authorization remote code execution flaw.

10.0 **CVE-2026-35431** Microsoft entra id

Server-side request forgery (ssrf) in Microsoft Entra ID Entitlement Management allows an unauthorized attacker to perform spoofing over a network.

9.8 **CVE-2026-31533** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net/tls: fix use-after-free in -EBUSY error path of tls_do_encryption The -EBUSY handling in tls_do_encryption(), introduced by commit 859054147318 ("net: tls: handle backlogging of crypto req

9.6 **CVE-2026-6919** Google chrome

Use after free in DevTools in Google Chrome prior to 147.0.7727.117 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-6920** Google chrome

Out of bounds read in GPU in Google Chrome on Android prior to 147.0.7727.117 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.3 **CVE-2026-33102** Microsoft 365 copilot

Url redirection to untrusted site ('open redirect') in M365 Copilot allows an unauthorized attacker to elevate privileges over a network.

9.8 **CVE-2026-6942** Radare radare2 mcp server

radare2-mcp version 1.6.0 and earlier contains an os command injection vulnerability that allows remote attackers to execute arbitrary commands by bypassing the command filter through shell metacharacters in user-controlled input passed to r2_cmd_str(). Attack

10.0 **CVE-2026-41196** Minetest minetest

Luanti (formerly Minetest) is an open source voxel game-creation platform. Starting in version 5.0.0 and prior to version 5.15.2, a malicious mod can trivially escape the sandboxed Lua environment to execute arbitrary code and gain full filesystem access on th

10.0 **CVE-2026-41211** Voidzero vite\+

Vite+ is a unified toolchain and entry point for web development. Prior to version 0.1.17, `downloadPackageManager()` accepts an untrusted `version` string and uses it directly in filesystem paths. A caller can supply `../` segments or an absolute path to esca

10.0 **CVE-2026-41679** Paperclip paperclipai DETECTION

Paperclip is a Node.js server and React UI that orchestrates a team of AI agents to run a business. Prior to version 2026.416.0, an unauthenticated attacker can achieve full remote code execution on any network-accessible Paperclip instance running in `authent

10.0 **CVE-2026-33819** Microsoft bing

Deserialization of untrusted data in Microsoft Bing allows an unauthorized attacker to execute code over a network.

9.9 **CVE-2026-41228** Froxlor froxlor

Froxlor is open source server administration software. Prior to version 2.3.6, the Froxlor API endpoint `Customers.update` (and `Admins.update`) does not validate the `def_language` parameter against the list of available language files. An authenticated custo

9.9 **CVE-2026-39440**

Improper Control of Generation of Code ('Code Injection') vulnerability in Funnelforms LLC FunnelFormsPro allows Remote Code Inclusion.This issue affects FunnelFormsPro: from n/a through 3.8.1.

9.9 **CVE-2026-40470**

A critical XSS vulnerability affected hackage-server and hackage.haskell.org. HTML and JavaScript files provided in source packages or via the documentation upload facility were served as-is on the main hackage.haskell.org domain. As a consequence, when a user

9.9 **CVE-2026-40472**

In hackage-server, user-controlled metadata from .cabal files are rendered into HTML href attributes without proper sanitization, enabling stored Cross-Site Scripting (XSS) attacks.

9.8 **CVE-2026-29198** Rocket.Chat rocket.chat

In Rocket.Chat <8.3.0, <8.2.1, <8.1.2, <8.0.3, <7.13.5, <7.12.6, <7.11.6, and <7.10.9, a NoSQL injection vulnerability can lead to account takeover of the first user with a generated token when an OAuth app is configured.

9.8 **CVE-2026-41176** Rclone rclone DETECTION

Rclone is a command-line program to sync files and directories to and from different cloud storage providers. The RC endpoint `options/set` is exposed without `AuthRequired: true`, but it can mutate global runtime configuration, including the RC option block i

9.8 **CVE-2026-41179** Rclone rclone DETECTION

Rclone is a command-line program to sync files and directories to and from different cloud storage providers. Starting in version 1.48.0 and prior to version 1.73.5, the RC endpoint `operations/fsinfo` is exposed without `AuthRequired: true` and accepts attack

9.8 **CVE-2026-3844** DETECTION

The Breeze Cache plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'fetch_gravatar_from_remote' function in all versions up to, and including, 2.4.4. This makes it possible for unauthenticated attackers to

9.8 **CVE-2026-3960** H2o h2o

A critical remote code execution vulnerability exists in the unauthenticated REST API endpoint /99/ImportSQLTable in H2O-3 version 3.46.0.9 and prior. The vulnerability arises due to insufficient security controls in the parameter blacklist mechanism, which on

25 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.