Daily brief, Thursday, July 23, 2026

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

Generated Nov 3, 2026, 10:15 AM ET

0	0	0	54	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

54 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

54

10.0 **CVE-2026-59555**

Unauthenticated Arbitrary File Deletion in Participants Database <= 2.7.8.3 versions.

10.0 **CVE-2026-64812** Jetbrains intellij idea

In JetBrains IntelliJ IDEA before 2026.2 unauthorized input injection was possible in a Remote Development session

10.0 **CVE-2026-64813** Jetbrains intellij idea

In JetBrains IntelliJ IDEA before 2026.2 unauthorized settings modification was possible in a Remote Development session

10.0 **CVE-2026-47668** DETECTION

DbGate is cross-platform database manager. In versions 7.1.8 and prior, DbGate's JSON script runner (`POST /runners/start`) allows remote code execution via code injection in the `functionName` parameter of JSON script `assign` commands. The `functionName` val

10.0 **CVE-2026-6516**

Zohocorp ManageEngine ADAudit Plus versions before 8606 are affected by Unauthenticated Remote code execution due to the vulnerable agent API.

10.0 **CVE-2025-71389**

Cal.com (calcom/cal.diy) before 5.9.9 is vulnerable to unauthenticated remote code execution because it bundles a version of Next.js whose React Server Components (RSC) request handling deserializes attacker-controlled input. A remote attacker can send a craft

10.0 **CVE-2026-42933**

Pronetiqs IntraVUE versions 3.2.1a14 and prior have an unintended proxy or intermediary vulnerability which could allow an attacker to use an active proxy, which would bypass OT segmentation.

9.9 **CVE-2026-59543**

Subscriber Remote Code Execution (RCE) in Advanced Views <= 3.8.11 versions.

9.9 **CVE-2026-44210** Katacontainers kata containers

Kata Containers is an open source project focusing on a standard implementation of lightweight Virtual Machines (VMs) that perform like containers. Versions prior to 3.31.0 ship with a default configuration that allows pod creators to inject arbitrary command-

9.9 **CVE-2026-47752**

Tugtainer is a self-hosted app for automating updates of Docker containers. Versions prior to 1.30.2 are vulnerable to Server-Side Template Injection (SSTI) in the notification template feature. The `title_template` and `body_template` fields are rendered usin

9.9 **CVE-2026-15630**

A non-global organization admin in one tenant can bypass tenant boundaries to delete, create, or modify resources in any other tenant by exploiting a mismatch between authorization (based on ?id=) and action (based on request body).

9.9 **CVE-2026-47724**

nebula-mesh is a self-hosted control plane for Slack Nebula mesh virtual private network. Prior to version 0.3.4, the `/api/v1/*` route surface trusts the bearer token alone for authorisation on most endpoints. The codebase itself admits this at `internal/api/

9.9 **CVE-2024-58354**

cal.com (calcom repository, later renamed cal.diy) is affected by a repository takeover vulnerability in its GitHub Actions workflows. The workflow pr.yml uses the pull_request_target trigger with the repository's default write permissions and passes them down

9.9 **CVE-2026-63732**

9router 0.4.59 (fixed in 0.4.60) contains a chain of vulnerabilities: a hardcoded default password (123456) that authenticates any fresh installation, a bypass of the LOCAL_ONLY network gate via a spoofed Host header, and unvalidated arguments passed to child_

9.8 **CVE-2026-14282**

The GoDAM – Organize WordPress Media Library & File Manager with Unlimited Folders for Images, Videos & more plugin for WordPress is vulnerable to arbitrary file uploads in versions up to, and including, 1.12.2. This is due to insufficient file type validation

9.8 **CVE-2026-15011**

The Customer Support Ticket System & Helpdesk plugin for WordPress is vulnerable to Code Injection via the 'path' parameter in all versions up to, and including, 6.0.5 due to the use of dynamic function invocation on an attacker-controlled value with insuffici

9.8 **CVE-2026-15015** DETECTION

The MountDev AI MCP Connector for WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.6.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it p

9.8 **CVE-2026-64873**

Joomla Extension - regularlabs.com - SSRF in Cache Cleaner Pro extension - Custom query URLs could access internal or reserved network services.

9.8 **CVE-2026-64874**

Joomla Extension - regularlabs.com - CDN Credential leakage Cache Cleaner Pro extension - CDN credentials were exposed in administrator request URLs.

9.8 **CVE-2026-65431**

Joomla Extension - regularlabs.com - Zipslip in GeoIP extension - Geo IP database update archives have been broadly extracted without path validation, leading to unsafe file extractions.

34 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. CVE IDs link to the full record on Watch Floor.