Daily brief, Friday, July 17, 2026

Jul 16, 8:00 PM to Jul 17, 8:00 PM ET

Generated Nov 3, 2026, 3:38 PM ET

0	0	0	30	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

30 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

30

10.0 **CVE-2026-54159**

PrestaShop ps_facetedsearch is a module that adds layered navigation filters. From 3.0.0 until 4.0.4, the ps_facetedsearch module rebuilds selected search filters from the request URL, and the value of a slider filter, price or weight, is taken from the URL wi

9.9 **CVE-2026-9135** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.10.0 Langflow versions up to 1.9.2 (commit 94981c443d4918517b9e8163d70fc598dc33a32d) contain a code injection vulnerability in the Policies component's ToolGuard integration that bypasses the allow_custom_components=false secur

9.9 **CVE-2026-8476** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.10.0 contain a critical remote code execution vulnerability in the disk-based caching mechanism. The AsyncDiskCache class uses Python's unsafe pickle.loads() function to deserialize cached objects from disk without validation,

9.9 **CVE-2026-8481** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.10.0 contain a critical remote code execution vulnerability in the code validation API endpoint. The POST /api/v1/validate/code endpoint accepts user-supplied Python code and executes it directly using Python's built-in exec()

9.9 **CVE-2026-8635** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.10.0 allows authenticated users to escalate privileges to superuser by directly manipulating the database, execute arbitrary system commands, and achieve full system compromise with Langflow service permissions.

9.9 **CVE-2026-8859** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.10.0 Langflow could allow an attacker to write arbitrary files to unintended locations due to improper input validation in the APIRequest component. A path traversal vulnerability exists when the "Save to File" feature is enabl

9.8 **CVE-2026-14956**

The Bricksforge plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.1.8.6. This is due to improper validation of the fieldIds parameter in the Pro Forms registration action, which allows attacker-supplied field ID

9.8 **CVE-2026-15982**

The Aimogen Pro - All-in-One AI Content Writer, Editor, ChatBot & Automation Toolkit plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.8.4. This is due to due to a missing capability check on the 'aiomatic_call_

9.8 **CVE-2026-9810**

The AI Copilot WordPress plugin before 1.5.4 does not bind OAuth access tokens to a WordPress user, and accepts any valid token as an administrator session, allowing unauthenticated attackers who complete the public OAuth flow to execute privileged MCP tools a

9.8 **CVE-2026-51080** Proxmox libpve-storage-perl

libpvestorage-perl v9.1.1 and libpve-storage-perl v8.3.7 were discovered to contain an XML External Entity (XXE) vulnerability.

9.8 **CVE-2026-60024**

Joomla Extension - joomdonation.com - Insecure default configuration Events Booking < 5.8.0 - The Joomla extension Events Booking prior version 5.8.0 did by default allow unauthenticated users to upload media assets.

9.8 **CVE-2026-12692**

Unverified password change vulnerability in Vimesoft Inc. Enterprise Video Platform allows Authentication Bypass. This issue affects Enterprise Video Platform: from 3.11.0.0 before 3.25.0.

9.8 **CVE-2026-8297**

Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Gis Informatics Engineering Consulting Laboratory R&D and Software Services Inc. GisLab Laboratory Management System allows SQL Injection. This issue affects

9.8 **CVE-2026-9202** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.10.0 allows unauthenticated attackers to create unlimited user accounts on any Langflow instance; when NEW_USER_IS_ACTIVE=true (documented deployment option), newly created accounts are immediately active and can authenticate t

9.8 **CVE-2026-9103** Langflow langflow DETECTION

IBM Langflow OSS 1.0.0 through 1.10.0 could allow a remote attacker to gain unauthorized access due to improper authentication in the /api/v1/login/auto_login endpoint. The endpoint issues long-lived superuser bearer tokens without requiring authentication whe

9.8 **CVE-2026-36669**

An unauthenticated arbitrary file upload vulnerability in ck_upload_handler.php in Feng Office 3.11.13.11 allows remote attackers to upload malicious files (such as .html) to the web-accessible /tmp/ directory.

9.8 **CVE-2026-8505** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.10.0 has a vulnerability in Langflow's webhook authentication logic allows unauthenticated users to trigger the execution of any flow. The system incorrectly bypasses API key validation when the WEBHOOK_AUTH_ENABLE configuratio

9.8 **CVE-2026-13446** Langflow langflow

IBM Langflow OSS 1.0.0 through 1.10.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.

9.8 **CVE-2026-48062**

CodeIgniter is a PHP full-stack web framework. Prior to 4.7.3, the ext_in upload validation rule in system/Validation/StrictRules/FileRules.php checked the MIME-derived guessed extension instead of the client-provided filename extension. As a result, an upload

9.8 **CVE-2026-52348**

cool-admin-java 8.0.0 has a SQL injection vulnerability in the order() method of CrudOption.java.

10 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.