Daily brief, Tuesday, July 7, 2026

Jul 6, 8:00 PM to Jul 7, 8:00 PM ET

Generated Nov 4, 2026, 12:45 AM ET

0	4	0	22	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 22 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

10.0 **CVE-2026-48282** Adobe ColdFusion CISA KEV DETECTION

An attacker can gain unrestricted file access and potentially execute code on an Adobe ColdFusion server.

10.0 **CVE-2026-48908** JoomShaper SP Page Builder CISA KEV DETECTION

An attacker can upload and execute arbitrary PHP code on a JoomShaper SP Page Builder server without authentication.

8.4 **CVE-2026-55255** Langflow Langflow CISA KEV

An authenticated attacker gains unauthorized access to other users' flows in Langflow.

9.8 **CVE-2026-56290** Joomlack Page Builder CISA KEV DETECTION

CVE published Jun 29, 2026

Joomla Extension - joomlack.fr - Unauthenticated file upload in Page Builder CK extension < 3.6.0 - The Joomla extension Page Builder CK is vulnerable to an unauthenticated arbitrary file upload that allows uploading executable files and leads to full RCE.

New public exploit code

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

New critical CVEs

22

10.0 **CVE-2026-48908** JoomShaper SP Page Builder KEV EXPLOIT CODE DETECTION

An attacker can upload and execute arbitrary PHP code on a JoomShaper SP Page Builder server without authentication.

10.0 **CVE-2026-48282** Adobe ColdFusion KEV EXPLOIT CODE DETECTION

An attacker can gain unrestricted file access and potentially execute code on an Adobe ColdFusion server.

9.9 **CVE-2026-34037**

+2 more CVEs in the same release

Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.464, the cloneTo() Livewire action in ResourceOperations.php authorizes the source resource but resolves destination resources with unscoped

9.8 **CVE-2026-12375**

The uncanny-automator-pro WordPress plugin before 7.3.0.6 was distributed with malicious code after the vendor's uncanny-automator-pro WordPress plugin before 7.3.0.6 update/distribution infrastructure was compromised; the injected backdoor grants unauthentica

9.8 **CVE-2026-14345**

The WPFunnels – Funnel Builder for WooCommerce with Checkout & One Click Upsell plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 3.12.7 via the 'postData' parameter parameter. This is due to unsanitized write of

9.8 **CVE-2026-33264** Apache airflow

A bug in `BaseSerialization.deserialize()` allowed unrestricted `import_string()` of attacker-controlled class paths when the Scheduler / API Server loaded a serialized DAG: a DAG author could embed a malicious trigger into a DAG to gain remote code execution

9.8 **CVE-2011-10043**

Module::Load versions before 0.22 for Perl allow arbitrary modules outside of @INC to be loaded. Module names starting with "::" could be passed to the load function to specify arbitrary module paths. Attackers able to influence module names passed to load cou

9.8 **CVE-2026-53481** Dell data domain operating system

+1 more CVEs in the same release

Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper limitation of a pathname to

9.8 **CVE-2026-13019** Esri portal for arcgis

Esri Portal for ArcGIS versions 12.1 and earlier on Windows, Linux and Kubernetes have a missing authentication for critical function vulnerability allows a remote, unauthenticated attacker to access an unprotected API. The following versions are known to be a

9.8 **CVE-2026-59800**

9Router before 0.4.44 contains an OS command injection vulnerability in the unauthenticated POST /api/tunnel/tailscale-install endpoint (this route is not covered by the dashboard middleware matcher, so no authorization check is applied). The sudoPassword fiel

9.8 **CVE-2026-14739** Perl dbi

DBI versions before 1.650 for Perl have a heap overflow when preparsing SQL statements with an extreme number of placeholders. The fix for CVE-2026-10879 did not allocate enough memory to handle approximately 1.2-million placeholders. DBI version 1.650 sets a

9.8 **CVE-2026-37270**

Trueview Security camera T18161- AF v4.9.60.0 contains an authentication bypass vulnerability caused by improper password validation and the presence of hard-coded credentials in the firmware.

9.8 **CVE-2026-37271**

Fire-Boltt Smartwatch FB BGS001 Firmware: MOY-JS14-2.0.4 is vulnerable to Improper Authentication, The device accepts GATT Write Request commands without sufficient authentication or strong session validation. Under specific conditions, previously captured BLE

9.8 **CVE-2026-59705**

mem0's openmemory/api component contains an unauthenticated access vulnerability that allows unauthenticated attackers to read, write, and delete arbitrary user memories by accessing API routers registered without authentication middleware. Attackers can suppl

9.3 **CVE-2026-59706**

mem0 contains unauthenticated config API endpoints that expose LLM API keys in plaintext and allow server-side request forgery via attacker-controlled ollama_base_url parameter. Unauthenticated attackers can retrieve stored secrets like OpenAI API keys via GET

9.1 **CVE-2026-58473**

Cognee before 1.2.0 contains an improper access control vulnerability that allows unauthenticated attackers to overwrite the global LLM provider configuration by self-registering an account and calling the settings endpoint, which performs no admin or superuse

9.1 **CVE-2026-46354** Coder coder

Coder allows organizations to provision remote development environments via Terraform. In versions prior tp 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3, `azureidentity.Validate()` verifies that the PKCS#7 signer certificate chains to a trusted Azure C

9.1 **CVE-2026-14740** Perl dbi

DBI versions before 1.650 for Perl read one byte out-of-bounds in preparse when deleting an initial SQL comment. The preparse method normalises SQL and removes comments. When the SQL starts with a comment line, the deletion of that line during normalisation le

9.0 **CVE-2026-4375**

The DoLeads Integrator WordPress plugin through 0.65, wp2epub WordPress plugin through 0.65 have been seen to be used to achieve RCE, once they are added adding to a blog, for example using a vulnerability where unclosed extensions from wordpress.org can be in

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.