Daily brief, Friday, June 26, 2026

Jun 25, 8:00 PM to Jun 26, 8:00 PM ET

Generated Nov 4, 2026, 10:51 AM ET

0	0	0	43	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

43 new critical CVEs, 1 new breaches.

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

43

9.3 **CVE-2026-56062** Oooorgle Quotes llama EXPLOIT CODE DETECTION

Unauthenticated SQL Injection in Quotes llama <= 3.1.5 versions.

9.8 **CVE-2026-48930** Nodejs node.js

A flaw in Node.js TLS hostname handling can cause Embedded-nul hostnames can lead to silent authority rebinding due to c-string truncation in resolver bindings. This vulnerability affects all supported release lines: **Node.js 22**, **Node.js 24**, and **Node.

9.8 **CVE-2026-53309** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ocfs2/dlm: fix off-by-one in dlm_match_regions() region comparison The local-vs-remote region comparison loop uses '<=' instead of '<', causing it to read one entry past the valid range of qr_

9.3 **CVE-2026-56070** ThemeHunk Advance Product Search DETECTION

Unauthenticated SQL Injection in Advance Product Search <= 1.4.4 versions.

9.8 **CVE-2026-0685** Edgewall *Genshi* Genshi
Server side template inject (SSTI) in the expression evaluation component in Genshi Template Engine version 0.7.9 allows a remote attacker to achieve remote code execution (RCE) via crafted template expressions.

9.8 **CVE-2026-56032** BuddyBoss Buddyboss Platform
Subscriber PHP Object Injection in Buddyboss Platform <= 3.0.4 versions.

9.8 **CVE-2026-56057** Uncanny Owl Uncanny Automator Pro
Subscriber PHP Object Injection in Uncanny Automator Pro <= 7.3.0.6 versions.

9.8 **CVE-2026-56030** Paytiumsupport Paytium
Unauthenticated Privilege Escalation in Paytium <= 5.0.2 versions.

9.8 **CVE-2026-56033** Dokan Multivendor Plugin Dokan Pro
Unauthenticated Privilege Escalation in Dokan Pro <= 5.0.4 versions.

9.9 **CVE-2026-56027** Pluggabl Booster for WooCommerce
Customer Arbitrary File Upload in Booster for WooCommerce <= 8.0.1 versions.

9.9 **CVE-2026-56058** ThemeCatcher Quform
Subscriber Arbitrary File Upload in Quform <= 2.23.0 versions.

9.9 **CVE-2026-56059** PhysCode Travel Booking
Subscriber Arbitrary File Upload in Travel Booking <= 2.2.5 versions.

9.3 **CVE-2026-56067** Crocoblock. Jetimpex JetSmartFilters
Unauthenticated SQL Injection in JetSmartFilters <= 3.8.3 versions.

9.3 **CVE-2026-56034** Online Web Tutor Library Management System
Unauthenticated SQL Injection in Library Management System <= 3.5.7 versions.

9.3 **CVE-2026-56036** Codemstory ????? ?? ????
Unauthenticated SQL Injection in ????? ?? ???? <= 5.5.6 versions.

9.3 **CVE-2026-56068** Crocoblock. Jetimpex JetEngine
Unauthenticated SQL Injection in JetEngine <= 3.8.10.2 versions.

10.0 **CVE-2026-54350** Budibase budibase
Budibase is an open-source low-code platform. Prior to 3.39.12, an unauthenticated visitor of any published Budibase app reads every document of the backing MongoDB, CouchDB, Elasticsearch, DynamoDB-PartiQL, or REST-with-JSON-body collection and, where the bui

10.0 **CVE-2026-53576** Kestra kestra **DETECTION**
Kestra is an open-source, event-driven orchestration platform. Prior to 1.0.45 and 1.3.21, the authentication filter for the REST API (@Filter("/api/v1/**")) treats any request whose path ends in /configs as the public instance-config endpoint and forwards it

9.9 **CVE-2026-46386**

OpenProject is open-source, web-based project management software. Prior to , the official openproject/openproject Docker image ships ENV SECRET_KEY_BASE=OVERWRITE_ME as the default Rails master key. Combined with cookies_serializer = :marshal, this gives any

9.9 **CVE-2026-52782**

OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, there is an IDOR through /projects/<A>/settings/project_storages/<A_ps_id> via PATCH parameter "storages_project_storage[project_folder_id]" leads to Access to Unaut

23 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

American Tower americantower.com 216,601 accounts

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.