# Daily brief, Thursday, August 6, 2026

Aug 5, 8:00 PM to Aug 6, 8:00 PM ET

Generated Nov 2, 2026, 8:44 PM ET

| 0 | 0 | 0 | 72 | 0 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

72 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

72

**9.6** **CVE-2026-19175** Google Chrome

Product not on watchlist.

**9.6** **CVE-2026-19149** Google chrome

Use after free in Aura in Google Chrome on Linux prior to 151.0.7922.109 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

**9.6** **CVE-2026-19157** Google chrome

Out of bounds write in ANGLE in Google Chrome on Android prior to 151.0.7922.109 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

**9.6** **CVE-2026-19164** Google chrome

Insufficient validation of untrusted input in Codecs in Google Chrome prior to 151.0.7922.109 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

**9.6** **CVE-2026-19166** Google chrome

Use after free in Web Authentication in Google Chrome prior to 151.0.7922.109 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-19170** Google chrome

Use after free in WebGL in Google Chrome on Android prior to 151.0.7922.109 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-19171** Google chrome

Use after free in Media in Google Chrome on Windows prior to 151.0.7922.109 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

10.0 **CVE-2026-65553**

Unauthenticated Remote Code Execution (RCE) in Spider Analyser – WordPress?????????? <= 2.1.3 versions.

10.0 **CVE-2026-66665**

Unauthenticated Arbitrary File Upload in Type Hub <= 2.0.6 versions.

10.0 **CVE-2026-11976**

The official MonsterInsights Pro update distribution bucket (`monster-insights.s3.amazonaws.com`) was compromised. Both the current release (10.2.2) and the version MonsterInsights rolled back to (10.2.0) contain a malicious file, `class-system-check.php`. Thr

10.0 **CVE-2026-14812**

The Premium SEO WordPress plugin is malicious: it ships an unauthenticated backdoor that creates a hidden administrator account and, in some builds, also enables remote code execution, server-side request forgery and arbitrary front-end script/content injectio

9.9 **CVE-2026-65548**

Contributor Remote Code Execution (RCE) in Betheme <= 28.4.2 versions.

9.9 **CVE-2026-48086**

**+3 more CVEs in the same release**

OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.2, a TENANT_ADMIN promotes themselves to platform-wide GLOBAL_ADMIN through a single PUT request. The role-update handler accepts t

9.9 **CVE-2026-67622** Flowiseai flowise

Flowise through 3.1.4 contains an insecure direct object reference vulnerability in the OpenAI Assistants integration that allows authenticated attackers to access credentials belonging to other workspaces by supplying an arbitrary credential UUID to Assistant

9.8 **CVE-2026-52466**

Open Library Foundation VuFind v11.0.3 and v4.1 is vulnerable to toInorrect Access Control. The application fails to stop processing an incoming request in VuFind\Controller\AbstractBase::validateAccessPermission after it has found that controller level access

9.8 **CVE-2026-67870**

In open62541 v1.5.5, the server-side AddReferences implementation contains an incomplete validation flaw for non-local ExpandedNodeId targets. A remote attacker can send a crafted AddReferencesRequest with an empty targetServerUri and a non-zero targetNodeId.s

9.8 **CVE-2026-67873**

A heap-based buffer overflow exists in lib60870-C 2.4.0 in the server-side FileSegment ASDU encoding path. The issue occurs because FileSegment_encode() validates only the standalone segment length via FileSegment_GetMaxDataSize() and does not verify the resid

9.8 **CVE-2026-1728** Wso2 api control plane

Tokens issued to a low-privileged user are not sufficiently restricted, allowing them to be used to access product-level Admin REST APIs. Exploitation of this vulnerability allows a low-privileged user to invoke the Admin REST APIs of WSO2 products, potentiall

9.8 **CVE-2026-64597**

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix double-free in SMB2_close() replay A response-bearing attempt can return a replayable error and free its response buffer. If SMB2_close_init() fails before the next send, clea

9.8 **CVE-2026-66909** Apache cxf

Apache CXF's JMS transport deserializes the body of any inbound JMS ObjectMessage using native Java deserialization, with no type restrictions in place. Any attacker able to place a message on the service's JMS destination can submit a malicious serialized obj

*49 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.