Daily brief, Wednesday, July 8, 2026

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

Generated Nov 3, 2026, 11:45 PM ET

0	0	0	20	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

20 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

20

9.6 **CVE-2026-15113** Google chrome

Use after free in Autofill in Google Chrome on Android prior to 150.0.7871.115 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

10.0 **CVE-2026-54782**

CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF SAML 1.1 and SAML 2.0 token validation does not correctly resolve the issuer signing key or require signed tokens when IdentityConfi

9.9 **CVE-2026-56843**

Incorrect authorization in the XML-RPC API of WebPros Plesk before 18.0.78.4 allows a low-privileged authenticated customer to look up domains they do not own, because ownership is enforced only for certain lookup filters and schema validation is bypassed for

9.8 **CVE-2026-9701**

The Eventer plugin for WordPress is vulnerable to an insecure password reset mechanism in all versions up to, and including, 4.4.2. The plugin stores a plaintext copy of the password reset key in the `eventer_verification_code` user meta field when a user requ

9.8 **CVE-2026-12153**

The WP Learn Manager plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.1.8. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthentic

9.8 **CVE-2026-9695**

An Improper Authentication vulnerability affecting DELMIA Apriso from Release 2020 through Release 2026 could allow an attacker to gain privileged access to the server.

9.8 **CVE-2026-14454** Tonycoz imager

Imager versions before 1.033 for Perl treat unsigned EXIF IFD entry counts as signed. Imager mishandled large EXIF IFD entry count values, treating them as negative numbers. This could lead to an attempt to allocate a block nearly the size of the address space

9.8 **CVE-2026-8307**

Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Webbeyaz Web Design Mediküm Web allows SQL Injection. This issue affects Mediküm Web: through 08072026. NOTE: The vendor was contacted and it was learned that

9.8 **CVE-2026-58480**

Blocksy Companion Pro plugin for WordPress before 2.1.47 contains an unauthenticated arbitrary file upload vulnerability that allows attackers to upload executable files by bypassing extension validation in the save_attachments function exposed through the Adv

9.8 **CVE-2026-31309**

Improper authorization in the /tequilapi/config/user endpoint of Mysterium Node from v1.21.1-rc0 before v1.36.0 allows an unauthenticated attacker to arbitrarily overwrite the node's configuration and achieve a full node takeover via a crafted POST request.

9.8 **CVE-2026-44024** Fluentd fluentd

Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, Fluentd allows dynamically constructing file paths using the ${tag} placeholder, and insufficient validation of ${tag} in f

9.8 **CVE-2026-52200**

An issue in Generic OEM UZ801_v2.1 4G LTE Router V3.4.3 allows a remote attacker to execute arbitrary code via the /ajax web management API endpoint in MifiService.apk

9.6 **CVE-2026-15062**

SQL injection vulnerabilities in the Snowflake Snowpark Python SDK (snowpark-python) versions prior to 1.53.0 could allow authenticated low-privilege users to execute SQL beyond their authorization scope. An attacker could exploit these vulnerabilities by embe

9.3 **CVE-2026-59702**

repomix contains a server-side request forgery vulnerability in the POST /api/pack endpoint that allows unauthenticated attackers to make arbitrary outbound requests. The endpoint fails to properly validate http://, https://, and file:// URLs before passing th

9.1 **CVE-2026-14487**

The Simple Coherent Form plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the removeUploadDir function in all versions up to, and including, 2.4.13. This makes it possible for unauthenticated attackers t

9.1 **CVE-2026-41042** DETECTION

Unauthenticated callers can supply a malicious H2 JDBC URL through the testConnection API, which executes arbitrary Java code on the server via H2's INIT parameter. Vulnerability in Apache Gravitino. This issue affects Apache Gravitino: before 1.2.1. Users are

9.1 **CVE-2026-54061**

Dgraph is an open source distributed GraphQL database. Prior to version 25.3.5, Dgraph Alpha exposes the RPCs used for external snapshot import on the public gRPC port `:9080` without authentication or authorization. As a result, an unauthenticated network cli

9.1 **CVE-2026-9074** Ibm api connect

IBM API Connect 10.0.8.0 through 10.0.8.9 and 12.1.0.0 through 12.1.0.3 contains an unauthenticated SQL injection vulnerability in the password reset functionality.

9.1 **CVE-2026-55471** Hapifhir hl7 fhir core

HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.10, org.hl7.fhir.utilities.XsltUtilities saxonTransform(...) overloads instantiated a bare net.sf.saxon.TransformerFactoryImpl() without ACCES

9.0 **CVE-2026-54527** Jupyter jupyterlab-git

JupyterLab Git is a Git extension for JupyterLab. From 0.30.0b3 before 0.54.0, the PlainTextDiff.ts createHeader() method passes Git filenames directly to innerHTML when rendering renamed files in commit history, allowing a crafted filename to execute JavaScri

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.