Daily brief, Wednesday, August 5, 2026

Aug 4, 8:00 PM to Aug 5, 8:00 PM ET

Generated Nov 2, 2026, 9:44 PM ET

0	1	0	51	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 51 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2026-63077** JetBrains TeamCity CISA KEV DETECTION

An attacker gains remote code execution on JetBrains TeamCity without authentication.

New public exploit code

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

New critical CVEs

51

9.8 **CVE-2026-63077** JetBrains TeamCity KEV EXPLOIT CODE DETECTION

An attacker gains remote code execution on JetBrains TeamCity without authentication.

9.8 **CVE-2026-20272** Cisco Cisco IOS XE Software

+1 more CVEs in the same release

Cisco IOS XE Software is affected. An attacker gains arbitrary code execution and remote command execution. Upgrade to the latest software version to address the vulnerabilities.

9.1 **CVE-2026-17556** GitHub enterprise server

A path traversal vulnerability was identified in GitHub Enterprise Server that allowed an unauthenticated attacker to delete arbitrary files and directories on the instance, including the entire user storage directory containing Git LFS objects, release assets

10.0 **CVE-2026-16940**

The Custom Fields WordPress plugin before 1.5.1 does not validate a user-supplied file path before deletion, allowing unauthenticated users to delete arbitrary files on the server (such as wp-config.php), which can lead to a full site takeover.

10.0 **CVE-2026-48168**

PraisonAI is a multi-agent teams system. In versions prior to 4.6.40, the bundled Claude GitHub Actions workflow is vulnerable to command injection because it embeds an attacker-controlled pull request branch name into a Bash run: block without quoting or vali

9.9 **CVE-2026-71268**

OpenPLC Runtime v3's compile_program function (webserver/openplc.py) parses directives from uploaded Structured Text (.st) program files and writes the referenced content to with no validation that file_path stays within the ./core directory. A path-validation

9.9 **CVE-2026-7329** Progress marklogic server

An improper privilege management vulnerability in the SQL, SPARQL, and Optic REST query interfaces of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an authenticated user with a low-privileged REST role to escalate privileges to administrator. This

9.9 **CVE-2026-8709** Progress marklogic server

An improper privilege management vulnerability in the REST API document patch operation of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an authenticated user with a low-privileged REST role to escalate privileges and execute privileged operations

9.9 **CVE-2026-9193** Progress marklogic server

An improper privilege management vulnerability in the Hadoop integration of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an authenticated user with a low-privileged Hadoop role to escalate privileges and execute privileged operations against the S

9.9 **CVE-2026-20303**

+2 more CVEs in the same release

As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Catalyst SD-WAN engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple intern

9.9 **CVE-2026-70615**

boringproxy through 0.10.0 contains a newline injection vulnerability that allows authenticated low-privileged users with tunnel-creation permission to inject arbitrary lines into the server account's SSH authorized_keys file by supplying a percent-encoded new

9.8 **CVE-2026-61484** Apache lucy

** UNSUPPORTED WHEN ASSIGNED ** Deserialization of Untrusted Data vulnerability in Apache Lucy. This issue affects Apache Lucy: all versions. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find a

9.8 **CVE-2026-61486** Apache lucy

** UNSUPPORTED WHEN ASSIGNED ** Stack-based Buffer Overflow vulnerability in Apache Lucy. This issue affects Apache Lucy: all versions. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alte

9.8 **CVE-2026-64566**

In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: propagate SKBFL_SHARED_FRAG in iptfs_skb_add_frags() When iptfs_skb_add_frags() copies frag references from the source frag walk into a new SKB, it increments the page reference c

9.8 **CVE-2026-71207**

The Stock-Inventory-Management-System application's login.php assigns raw username/password values to and builds its authentication query by directly concatenating those session values into a SQL statement with no parameterization or escaping. The same script

9.8 **CVE-2026-71214**

The Aerie/PlanDev sequencing-server's authorization middleware (sequencing-server/src/app.ts) derives the caller's Hasura session role via getHasuraSession, which prefers a session_variables object taken directly from the client-supplied JSON request body over

9.8 **CVE-2026-66747** DETECTION

Zbtlink router firmware ships an embedded remote-control implant, ENDLESSDOORS, present in every published build across the product line. It is the open-source ycsunjane/rctl tool built in as an OpenWrt package (librctl.so), started at boot and run as root und

9.8 **CVE-2026-71231**

IOTSmartHome's gui/login.php checkCookie function builds an authentication query as SELECT * FROM users WHERE ID='<decoded lastLogin cookie>' after base64-decoding the client-supplied lastLogin cookie via safe_decode, which performs URL-safe base64 decoding wi

9.8 **CVE-2026-71237**

Miantang/IoT-PHP's index.php implements a POST /userlogin route that reads the password directly from ['pwd'] with no sanitization and concatenates it into a raw SQL string: mysql_query("select * from userlists where username='' and password='' limit 1"). An u

9.8 **CVE-2026-71248**

Inventory-Management-System-PHP's login.php constructs its authentication query via direct string concatenation of raw POST parameters: = "select * from user where email = '' and password = ''", with no escaping or parameterization, allowing authentication byp

28 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Inter-Con Security icsecurity.com 276,114 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.