Daily brief, Monday, July 6, 2026

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

Generated Nov 4, 2026, 1:30 AM ET

0	0	0	31	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

31 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

31

9.9 **CVE-2026-34038** Coollabsio coolify EXPLOIT CODE

Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.469, an authenticated remote command injection vulnerability in application deployment handling allows users with application write permissi

9.8 **CVE-2026-11405** Tenda firmware EXPLOIT CODE

The web server binary /bin/httpd contains a hidden backdoor authentication mechanism in the login() function at 004c88b8. - The function contains a normal authentication path using MD5/hash-based password verification (prod_encode64/PasswordToMd5/check_rand_ke

9.8 **CVE-2026-9181** Esri arcgis server DETECTION

Esri ArcGIS Server contains a directory traversal vulnerability. ArcGIS Enterprise on Kubernetes is not impacted. An unauthenticated attacker could exploit this issue by sending crafted path parameters. Successful exploitation could allow overwriting sensitive

10.0 **CVE-2026-48316** Adobe coldfusion

ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is

9.8 **CVE-2026-9182** Esri arcgis server

Esri ArcGIS Server contains an unrestricted file upload vulnerability. An unauthenticated attacker could exploit this issue by uploading a crafted file to the affected endpoint. Successful exploitation could allow arbitrary file upload, potentially allowing fo

9.9 **CVE-2026-48614** WebPros Plesk

An improper authorization vulnerability in the Plesk XML API allows an authenticated user to inject arbitrary configuration directives, resulting in arbitrary file write as root and full privilege escalation on the underlying server.

10.0 **CVE-2026-54763** Traefik traefik

Traefik is an HTTP reverse proxy and load balancer. Prior to v2.11.51, v3.6.22, and v3.7.6, Traefik's BasicAuth, DigestAuth, and ForwardAuth middlewares strip canonical-cased spoofed identity headers before writing Traefik's own value, but do not account for u

10.0 **CVE-2026-57572** Kidocode crawl4ai

Crawl4AI is an open-source LLM-friendly web crawler and scraper. Prior to 0.9.0, the Docker API server accepted request-supplied browser_config.extra_args, which flowed into Chromium's launch arguments. An attacker could inject Chromium switches that replace a

9.9 **CVE-2026-40141** Beyondtrust privileged remote access

A high-severity vulnerability exists in a web application component of BeyondTrust Remote Support and Privileged Remote Access related to the processing of certain input parameters. Insufficient validation of user-supplied input may allow an authenticated atta

9.8 **CVE-2026-14807**

ERP App developed by PROG MIS has a Use of Hard-coded Credentials vulnerability, allowing unauthenticated remote attackers to log in to view application code and obtain the database account and password.

9.8 **CVE-2026-14808**

Prog Management System developed by PROG MIS has a Exposure of Sensitive Information vulnerability, allowing unauthenticated remote attackers to view a specific page and obtain the database account and password.

9.8 **CVE-2026-24014** Apache iotdb

Apache IoTDB DataNode’s internal RPC interface for creating Trigger instances uses the uploaded Trigger JAR name to build a file path without sufficient validation. If the internal DataNode RPC port is exposed to an untrusted network, an attacker may use path

9.8 **CVE-2026-43867** Apache camel

Deserialization of Untrusted Data vulnerability in Apache Camel PQC Component. The camel-pqc component persists post-quantum key metadata (KeyMetadata) through pluggable KeyLifecycleManager implementations. AwsSecretsManagerKeyLifecycleManager.deserializeMetad

9.8 **CVE-2026-46454** Apache camel

Improper Input Validation vulnerability in Apache Camel Cometd Component. The camel-cometd component maps inbound Bayeux (CometD) message headers into the Camel Exchange without applying a HeaderFilterStrategy. CometdBinding.populateExchangeFromMessage copies

9.8 **CVE-2026-46455** Apache camel

Insufficient Session Expiration vulnerability in Apache Camel Keycloak Component. The camel-keycloak security helper KeycloakSecurityHelper.parseAndVerifyAccessToken builds a Keycloak TokenVerifier using withChecks(...) with only the subject-exists check and t

9.8 **CVE-2026-46456** Apache camel

Improper Input Validation vulnerability in Apache Camel AWS2-SQS Component. The camel-aws2-sqs component map inbound message attributes into the Camel Exchange through a component-specific HeaderFilterStrategy. Sqs2HeaderFilterStrategy configured only an outbo

9.8 **CVE-2026-48204** Apache camel

Improper Input Validation, Improper Access Control vulnerability in Apache Camel in Camel Mongodb Gridfs component. The camel-mongodb-gridfs producer selects the GridFS operation to perform from the gridfs.operation Exchange header when the endpoint's operatio

9.8 **CVE-2026-53913** Apache camel

Improper Authentication, Missing Authentication for Critical Function, Not Failing Securely ('Failing Open') vulnerability in Apache Camel Keycloak Component. The KeycloakSecurityPolicy of camel-keycloak guards a route by running KeycloakSecurityProcessor.befo

9.8 **CVE-2026-56140** Apache camel

Improper Input Validation vulnerability in Apache Camel AWS SNS component. The camel-aws2-sns component filters Camel headers through a component-specific HeaderFilterStrategy, Sns2HeaderFilterStrategy. Like the sibling Sqs2HeaderFilterStrategy, it originally

9.8 **CVE-2026-40139** Beyondtrust privileged remote access

A critical pre-authentication vulnerability exists in the authentication subsystem of BeyondTrust Remote Support. Improper processing of authentication requests may allow an unauthenticated remote attacker to bypass access controls and gain unauthorized access

11 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.