Daily brief, Monday, June 1, 2026

May 31, 8:00 PM to Jun 1, 8:00 PM ET

Generated Nov 5, 2026, 11:02 AM ET

0	1	0	20	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 20 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

7.5 **CVE-2024-21182** Oracle WebLogic Server CISA KEV

An attacker gains remote code execution and unauthorized access to sensitive data in Oracle WebLogic Server.

New public exploit code

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

New critical CVEs

20

10.0 **CVE-2026-45131**

+1 more CVEs in the same release

CloudPirates Open Source Helm Charts is a collection of Helm charts. Prior to commit fcf9302, a GitHub Actions workflow (pull-request.yaml) executes attacker-controlled code from fork pull requests in a privileged context, exposing repository secrets including

10.0 **CVE-2026-40965**

Cloud Foundry UAA versions v76.12.0 through v78.12.0 are vulnerable to a private key exposure. The server contains a vulnerability where EC (Elliptic Curve) private keys are inadvertently exposed through the public /token_keys endpoint. This endpoint is design

9.8 **CVE-2026-7858**

A Deserialization of Untrusted Data vulnerability affecting Teamwork Cloud from No Magic Release 2022x through No Magic Release 2026x and Magic Collaboration Studio from CATIA Magic Release 2022x through CATIA Magic Release 2026x could lead to an unauthenticat

9.8 **CVE-2026-42680**

Incorrect Privilege Assignment vulnerability in Wasiliy Strecker / ContestGallery developer Contest Gallery Pro allows Privilege Escalation. This issue affects Contest Gallery Pro: from n/a through 29.0.1.

9.8 **CVE-2026-48879**

Incorrect Privilege Assignment vulnerability in Sergey AIWU allows Privilege Escalation. This issue affects AIWU: from n/a through 1.4.17.

9.8 **CVE-2018-25427**

Arm Whois 3.11 contains a stack-based buffer overflow vulnerability that allows remote attackers to execute arbitrary code by supplying oversized input to the IP address or domain field. Attackers can craft malicious input exceeding 658 bytes with shellcode to

9.8 **CVE-2026-25879**

Langroid is a framework for building large-language-model-powered applications. Prior to version 0.63.0, SQLChatAgent executes SQL produced by an LLM, which is influenceable by prompt injection. When configured with a database role that has privileges enabling

9.6 **CVE-2026-48866**

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Rocketgenius Inc. Gravity Forms allows Path Traversal. This issue affects Gravity Forms: from n/a through 2.10.0.1.

9.6 **CVE-2026-44211** Cline cline

Cline is an autonomous coding agent as an SDK, IDE extension, or CLI assistant. In versions 2.13.0 and prior, there is a cross-origin WebSocket hijack vulnerability in Cline Kanban servers. At time of publication, there are no publicly available patches.

9.4 **CVE-2026-8931**

A critical Remote Code Execution (RCE) vulnerability exists in Disig Web Signer versions 2.0.3 through 2.5.3.

9.3 **CVE-2026-42672**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wp Directory Kit WP Directory Kit allows Blind SQL Injection. This issue affects WP Directory Kit: from n/a through 1.5.1.

9.2 **CVE-2026-0826** DETECTION

In certain scenarios when the admin has enabled Interactive Connectivity Establishment (ICE), a buffer overflow could enable remote code execution on Poly Voice products on the Linux platform.

9.1 **CVE-2026-48188** Otrs otrs

An improper Input Validation vulnerability in OTRS or ((OTRS)) Community Edition database layer module allows an unauthenticated SQL injection which can lead to an authentication bypass. This issue only affects the system if the MySQL/MariaDB server is configu

9.1 **CVE-2026-42252** Apache airflow

Apache Airflow's official documentation at `core-concepts/dag-run.html` ("Passing Parameters when triggering Dags") showed a verbatim `BashOperator(bash_command="echo value: {{ dag_run.conf['conf1'] }}")` example without any quoting / sanitization warning. Dag

9.1 **CVE-2026-42682**
Missing Authorization vulnerability in Tomdever wpForo Forum allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects wpForo Forum: from n/a through 3.0.6.

9.1 **CVE-2026-22872** Projectcapsule capsule
Capsule is a multi-tenancy and policy-based framework for Kubernetes. The Capsule Controller runs with cluster-admin privileges. Although the TenantResource RawItems processing logic forcibly sets the namespace, this is ineffective for cluster-scoped resources

9.1 **CVE-2026-8644** Ibm websphere application server
IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to identity spoofing.

9.0 **CVE-2026-9311** Ibm websphere application server
IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to remote code execution caused by the bypass of security controls.

9.0 **CVE-2026-9319** Ibm websphere application server
IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to potential remote code execution due to deserialization of untrusted data via JAX-WS endpoints with WS-Security.

Ransomware

No leak-site posts collected.

New data breaches 1

Edmunds edmunds.com 177,860 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.