Daily brief, Thursday, June 11, 2026

Jun 10, 8:00 PM to Jun 11, 8:00 PM ET

Generated Nov 5, 2026, 1:36 AM ET

0	1	0	19	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 19 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2026-10520** Ivanti Sentry CISA KEV DETECTION

An attacker gains remote code execution on Ivanti Sentry.

New public exploit code

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

New critical CVEs

19

10.0 **CVE-2026-10520** Ivanti Sentry KEV EXPLOIT CODE DETECTION

An attacker gains remote code execution on Ivanti Sentry.

10.0 **CVE-2026-49261** Mariadb mariadb

MariaDB server is a community developed fork of MySQL server. Versions 10.6.1 through 10.6.26, 10.11.1 through 10.11.17, 11.4.1 through 11.4.11, 11.8.1 through 11.8.7, and 12.3.1 with `wsrep_notify_cmd` enabled would execute shell commands embedded in the name

9.6 **CVE-2026-12027** Google chrome

Inappropriate implementation in Headless in Google Chrome prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.1 **CVE-2026-45177** Palo Alto Networks idira secrets manager edge

Idira Secrets Manager SaaS Edge versions prior to 1.8 exhibit improper access control within its internal authentication components. A remote, unauthenticated attacker could exploit this by submitting a specially crafted request. Under specific circumstances,

9.9 **CVE-2026-11839**

Unrestricted upload of file with dangerous type vulnerability in Ba?arsoft Information Technologies Inc. Rotaban allows Upload a Web Shell to a Web Server. This issue affects Rotaban: from V2026.06.002 before V2026.06.003.

9.8 **CVE-2026-11561**

Improper neutralization of special elements used in an expression language statement ('expression language injection') vulnerability in Soagen Informatics Technologies Software and Consulting Inc. Apinizer allows Code Injection. This issue affects Apinizer: fr

9.8 **CVE-2026-7852**

Unrestricted upload of file with dangerous type vulnerability in Limatek System Inc. LimRAD NAC allows Remote Code Inclusion. This issue affects LimRAD NAC: before 5.5.7.3.9.

9.8 **CVE-2026-38581**

SQL Injection vulnerability in damasac thaipalliative_lte through version 3.0 allows remote attackers to execute arbitrary SQL commands via the idFormMain parameter to /substudy/ezform.php (line 14) and the id parameter (line 49). The parameters are concatenat

9.8 **CVE-2026-49060** DETECTION

Incorrect Privilege Assignment vulnerability in Hippoo Mobile App for WooCommerce allows Privilege Escalation. This issue affects Hippoo Mobile App for WooCommerce: from n/a through 1.9.4.

9.8 **CVE-2026-42846**

ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 - #140, ClipBucket's Remote Play feature allows any authenticated user to add a video by importing an external URL as the source. Some shell commands are run with the URL as a param

9.8 **CVE-2026-45060**

ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 - #129, the actions/progress_video.php endpoint is vulnerable to blind SQL injection. Any unauthenticated user can exploit the ids parameter to execute SQL queries and exfiltrate se

9.5 **CVE-2026-47172**

Quest Bot is an opensource modern Discord Bot built for moderation, utilities and support. Prior to version 1.0.3, the repository has a privileged deploy workflow that runs after the unprivileged build workflow completes. The build workflow runs on pull reques

9.5 **CVE-2026-47174**

In Duck Site before version 1.0.1, the repository has a deploy workflow that runs after the build workflow completes. The build workflow runs on pull requests, while the deploy workflow runs with package-write permissions and deployment secrets. If an attacker

9.4 **CVE-2026-4764**

A Missing Authorization vulnerability in the playbook import functionality in Dialogflow CX on Google Cloud Platform allows an authenticated user with specific roles to escalate privileges and potentially take over a GCP project using a maliciously crafted pla

9.4 **CVE-2026-49973**

Hermes WebUI before version 0.51.358 contains an improper access control vulnerability that allows unauthenticated remote attackers to hijack initial setup by submitting the _set_password parameter to the settings API endpoint without any network origin restri

9.3 **CVE-2026-39494**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WBW Plugins Product Filter by WBW allows Blind SQL Injection. This issue affects Product Filter by WBW: from n/a through 3.1.2.

9.3 **CVE-2026-42647** DETECTION

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Beardev JoomSport allows Blind SQL Injection. This issue affects JoomSport: from n/a through 5.7.7.

9.1 **CVE-2026-9648**

The crypton-x509-validation Haskell library fails to enforce X.509 NameConstraints, allowing TLS clients to accept certificates whose Subject Alternative Names fall outside the issuing CA’s permitted subtrees. This oversight enables an attacker who compromises

9.0 **CVE-2026-41005**

Cloud Foundry UAA incorrectly treated XML encryption to the Service Provider (confidentiality) as a substitute for XML signatures from the Identity Provider (authenticity) in two SAML flows: the OAuth 2.0 SAML2 bearer grant (token endpoint) and browser SSO (AC

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.