Daily brief, Friday, June 12, 2026

Jun 11, 8:00 PM to Jun 12, 8:00 PM ET

Generated Nov 5, 2026, 12:40 AM ET

0	1	0	34	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 34 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2026-35273** Oracle PeopleSoft Enterprise PeopleTools CISA KEV DETECTION

An unauthenticated attacker gains takeover of PeopleSoft Enterprise PeopleTools with Oracle PeopleSoft Enterprise PeopleTools.

New public exploit code

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

New critical CVEs

34

9.8 **CVE-2026-35273** Oracle PeopleSoft Enterprise PeopleTools KEV EXPLOIT CODE DETECTION

An unauthenticated attacker gains takeover of PeopleSoft Enterprise PeopleTools with Oracle PeopleSoft Enterprise PeopleTools.

9.8 **CVE-2026-44170** Mariadb mariadb

MariaDB server is a community developed fork of MySQL server. From versions 10.6.1 to before 10.6.26, 10.11.1 to before 10.11.17, 11.4.1 to before 11.4.11, 11.8.1 to before 11.8.7, and 12.3.1, MariaDB on WIndows with installed CONNECT engine and enabled REST s

9.1 **CVE-2026-44172** Mariadb mariadb

MariaDB server is a community developed fork of MySQL server. In versions 3.3.18 and 3.4.8, an application that was taking non-validated user input, escaping it with mysql_real_escape_string() and sending it to the database using text protocol and big5 charact

9.8 **CVE-2026-49875** Apache cxf

Apache CXF's EndpointReferenceUtils and W3CMultiSchemaFactory classes construct a SAXParserFactory without the necessary JAXP hardening configurations, enabling out-of-band (OOB) external entity resolution. Users are recommended to upgrade to versions 4.2.2 or

10.0 **CVE-2026-47131**

vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, by combining Buffer.call.call({}.__lookupGetter__, Buffer, "__proto__"), Buffer.call.call({}.__lookupSetter__, Buffer, "__proto__"), and Node.js's ERR_INVALID_ARG_TYPE Error, the host's Typ

10.0 **CVE-2026-47137**

vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, the fix for GHSA-8hg8-63c5-gwmx (CVE-2023-37903) introduced a check in nodevm.js line 263 that blocks the combination nesting: true + require: false. However, the check uses strict equality

10.0 **CVE-2026-47140**

vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, NodeVM blocks several dangerous Node.js builtins such as module, worker_threads, cluster, vm, repl, and inspector. However, the denylist misses process and inspector/promises. Both can be u

10.0 **CVE-2026-47208**

vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, VM2 suffers from a sandbox breakout vulnerability. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This issue ha

10.0 **CVE-2026-50086** Aqara iam\/sso gateway

The Aqara IAM/SSO gateway (gw-builder.aqara.com) exposes bidirectional AES round-trups against the platform's signing key without authentication. This is an instance of "CWE-306: Missing Authentication for Critical Function" and "CWE-327: Use of a Broken or Ri

9.9 **CVE-2026-47365**

Argument injection vulnerability in WordPress Toolkit before 6.11.0 as used in cPanel & WHM, allows remote authenticated users to bypass cross-tenant authorization and execute arbitrary wp-toolkit CLI commands as another account.

9.9 **CVE-2026-47367**

+2 more CVEs in the same release

A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UID Enterprise Agent to execute a Command Injection on the host device.

9.9 **CVE-2026-46716**

Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 1.4.0 to before version 2.0.8, a RoleMember user can create a scheduled cron task with Cover=CronCoverAll, Servers=[] and an arbitrary Command. At ever

9.8 **CVE-2026-48611** DETECTION

Improper authentication checks in the OAuth implementation allow account hijacking even when OAuth is not configured or enabled leading to unauthorized access in default installations.

9.8 **CVE-2026-50628** Apache cxf

A logic error in OAuthRequestFilter rejects legitimate requests originating from the bound IP address, while blindly allowing requests from any other IP address. Enabling this security feature inadvertently creates an inverse security check. Users are recommen

9.8 **CVE-2026-11849**

The iRM-IEI Remote Management developed by IEI Integration Corp has a Hardcoded Credentials vulnerability, allowing unauthenticated remote attackers to exploit hard-coded credentials to gain administrative privileges on the database.

9.8 **CVE-2026-10557**

The Yarbo Android and iOS applications contain hard-coded MQTT broker credentials that are identical for all users and all devices. These credentials are embedded in the application binary and are readily extractable via APK decompilation. The credentials prov

9.8 **CVE-2026-47210**

vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, a sandbox escape vulnerability in vm2 allows arbitrary code execution in the host process when untrusted code is executed with async support on runtimes exposing WebAssembly JSPI (WebAssemb

9.8 **CVE-2026-53787** DETECTION

Amasty Order Attributes for Magento 2 before version 4.0.0 contains an unauthenticated arbitrary file upload vulnerability that allows unauthenticated attackers to write arbitrary files to the store's media directory by submitting files of any type or name to

9.8 **CVE-2026-54133** Jmespath jmespath

jmespath.php allows users to use JMESPath, software for declaratively specifying how to extract elements from a JSON document, in PHP applications with PHP data structures. Versions prior to 2.9.1 can generate and execute attacker-controlled PHP code when `Jme

9.8 **CVE-2026-6853**

Improper restriction of excessive authentication attempts vulnerability in Ba?belen Group Food Cafe Businesses Industry and Trade Ltd. Co. Pause+ Mobile App allows Authentication Bypass. This issue affects Pause+ Mobile App: from v1.0.6 before v1.5.

12 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.