Daily brief, Sunday, May 10, 2026

May 9, 8:00 PM to May 10, 8:00 PM ET

Generated Nov 7, 2026, 2:24 AM ET

0	0	0	9	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

9 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

9

9.8 **CVE-2025-14179** Php php

In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, the PDO Firebird driver improperly handles NUL bytes when preparing SQL queries. During token-by-token query construction, a string token containing a NUL by

9.8 **CVE-2026-6722** Php php

In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, the SOAP extension's object deduplication mechanism stores pointers to PHP objects in a global map without incrementing their reference counts. When an apach

9.8 **CVE-2026-7261** Php php

In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, when SoapServer is configured with SOAP_PERSISTENCE_SESSION, the handler object is persisted across requests via session storage. However, in the case SOAP r

9.1 **CVE-2026-6104** Php php

In PHP versions 8.4.* before 8.4.21 and 8.5.* before 8.5.6, when an encoding name containing an embedded NUL byte is passed to mb_convert_encoding() or related mbstring functions, the code incorrectly assumes that when strncasecmp() returns 0 it means the stri

9.8 **CVE-2021-47923**

OpenCart 3.0.3.8 contains a session fixation vulnerability that allows attackers to hijack user sessions by injecting arbitrary values into the OCSESSID cookie. Attackers can set malicious OCSESSID cookie values that the server accepts and maintains, enabling

9.8 **CVE-2021-47932**

WordPress TheCartPress 1.5.3.6 contains an unauthenticated privilege escalation vulnerability that allows attackers to create administrator accounts by submitting crafted requests to the AJAX handler. Attackers can send POST requests to the tcp_register_and_lo

9.8 **CVE-2021-47933**

WordPress MStore API 2.0.6 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious files by sending POST requests to the REST API endpoint. Attackers can upload PHP files with arbitrary names to the config_file

9.8 **CVE-2021-47936**

OpenCATS 0.9.4 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary commands by uploading malicious PHP files disguised as resume attachments. Attackers can upload PHP payloads through the careers job applic

9.8 **CVE-2021-47940**

WordPress Plugin Download From Files version 1.48 and earlier contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious files by exploiting the AJAX fileupload action. Attackers can send POST requests to the admi

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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.