Daily brief, Tuesday, May 5, 2026

May 4, 8:00 PM to May 5, 8:00 PM ET

Generated Nov 7, 2026, 3:22 AM ET

0	0	0	27	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

27 new critical CVEs, 1 new breaches.

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

27

9.8 **CVE-2026-43067** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ext4: handle wraparound when searching for blocks for indirect mapped blocks Commit 4865c768b563 ("ext4: always allocate blocks only from groups inode can use") restricts what blocks will be a

9.8 **CVE-2026-34084** Phpoffice phpspreadsheet

PhpSpreadsheet is a library for reading and writing spreadsheet files. In versions 1.30.2 and earlier, 2.0.0 through 2.1.14, 2.2.0 through 2.4.3, 3.3.0 through 3.10.3, and 4.0.0 through 5.5.0, when the filename argument to IOFactory::load() is user-controlled,

9.8 **CVE-2026-28780** Apache http server

Heap-based Buffer Overflow vulnerability in mod_proxy_ajp of Apache HTTP Server. If mod_proxy_ajp connects to a malicious AJP server this AJP server can send a malicious AJP message back to mod_proxy_ajp and cause it to write 4 attacker controlled bytes after

9.1 **CVE-2026-43071** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: dcache: Limit the minimal number of bucket to two There is an OOB read problem on dentry_hashtable when user sets 'dhash_entries=1': BUG: unable to handle page fault for address: ffff888b30b77

9.8 **CVE-2026-27960** OpenCTI-Platform opencti DETECTION

Product not on watchlist.

10.0 **CVE-2026-7411**

In Eclipse BaSyx Java Server SDK versions prior to 2.0.0-milestone-10, inadequate path normalization in the Submodel HTTP API allows an unauthenticated remote attacker to perform a path traversal attack. By supplying a maliciously crafted fileName parameter du

9.8 **CVE-2026-5722**

The MoreConvert Pro plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.9.14. This is due to the guest waitlist verification flow not invalidating or regenerating verification tokens when the customer email addre

9.8 **CVE-2025-13618**

The Mentoring plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.2.8. This is due to the plugin not properly restricting the roles that users can register with in the mentoring_process_registration() function. Th

9.8 **CVE-2026-5294**

The Geeky Bot plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.2.2. This is due to a nopriv AJAX route allowing attacker-controlled model/function dispatch and reaching a plugin installer helper that downloads and

9.8 **CVE-2026-7823**

A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. Affected is the function setAppFilterCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument enable results in os command injection. The attack may be launched remotely

9.8 **CVE-2023-54342**

Eclipse Equinox OSGi versions 3.8 through 3.18 contain a remote code execution vulnerability in the console interface that allows unauthenticated attackers to execute arbitrary code by exploiting the fork command functionality. Attackers can establish a telnet

9.8 **CVE-2023-54344**

Eclipse Equinox OSGi 3.7.2 and earlier contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary commands by sending payloads to the console interface. Attackers can connect to the OSGi console port and send base

9.8 **CVE-2026-7834**

A security vulnerability has been detected in EFM ipTIME NAS1dual 1.5.24. This issue affects the function get_csrf_whites of the file /cgi/advanced/misc_main.cgi. Such manipulation leads to stack-based buffer overflow. The attack can be launched remotely. The

9.8 **CVE-2026-38429**
OpenCMS v20 and before is vulnerable to XML External Entity (XXE) in the Admin Import DB feature due to insecure XML parsing of user supplied .zip files containing a manifest.xml.

9.8 **CVE-2026-38431** Frappe erpnext
ERPNext v15.103.1 and before is vulnerable to Server-Side Template Injection (SSTI). An attacker with permission to create or edit email templates can inject template expressions that are executed on the server when the template is rendered.

9.8 **CVE-2026-7853** Dlink di-8100 firmware DETECTION
A weakness has been identified in D-Link DI-8100 16.07.26A1. Affected is the function sprintf of the file /auto_reboot.asp of the component HTTP Handler. This manipulation of the argument enable/time causes buffer overflow. It is possible to initiate the attac

9.8 **CVE-2026-38428** Kestra kestra
Kestra v1.3.3 and before is vulnerable to SQL Injection. The vulnerability occurs because user-controlled input from a GET parameter is directly concatenated into an SQL query without proper sanitization or parameterization. As a result, attackers can inject a

9.8 **CVE-2026-7854** Dlink di-8100 firmware DETECTION
A security vulnerability has been detected in D-Link DI-8100 16.07.26A1. Affected by this vulnerability is the function url_rule_asp of the file /url_rule.asp of the component POST Parameter Handler. Such manipulation leads to buffer overflow. It is possible t

9.8 **CVE-2026-35579** Coredns.Io coredns
CoreDNS is a DNS server written in Go. In versions prior to 1.14.3, the gRPC, QUIC, DoH, and DoH3 transport implementations incorrectly handle TSIG authentication. For gRPC and QUIC, the server checks whether the TSIG key name exists in the configuration but n

9.3 **CVE-2026-40797**
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saleswonder LLC WebinarIgnition allows Blind SQL Injection. This issue affects WebinarIgnition: from n/a through 4.08.253.

7 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Vimeo vimeo.com 119,167 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. 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.