Daily brief, Tuesday, April 7, 2026

Apr 6, 8:00 PM to Apr 7, 8:00 PM ET

Generated Nov 7, 2026, 8:35 AM ET

0	0	0	45	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

45 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

45

9.8 **CVE-2026-1114** Parisneo parisneo/lollms EXPLOIT CODE

Product not on watchlist.

9.8 **CVE-2026-5731** Mozilla firefox

Memory safety bugs present in Firefox ESR 115.34.0, Firefox ESR 140.9.0, Thunderbird ESR 140.9.0, Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have b

9.8 **CVE-2026-5734** Mozilla firefox

Memory safety bugs present in Firefox ESR 140.9.0, Thunderbird ESR 140.9.0, Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run a

9.8 **CVE-2026-5735** Mozilla firefox

Memory safety bugs present in Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in

9.8 **CVE-2026-31789** Openssl openssl

Issue summary: Converting an excessively large OCTET STRING value to a hexadecimal string leads to a heap buffer overflow on 32 bit platforms. Impact summary: A heap buffer overflow may lead to a crash or possibly an attacker controlled code execution or other

9.8 **CVE-2026-0740** DETECTION

The Ninja Forms - File Uploads plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'NF_FU_AJAX_Controllers_Uploads::handle_upload' function in all versions up to, and including, 3.3.26. This makes it possible

9.8 **CVE-2026-22679** Weaver e-cology

Weaver (Fanwei) E-cology 10.0 versions prior to 20260312 contain an unauthenticated remote code execution vulnerability in the /papi/esearch/data/devops/dubboApi/debug/method endpoint that allows attackers to execute arbitrary commands by invoking exposed debu

9.8 **CVE-2026-4631** DETECTION

Cockpit's remote login feature passes user-supplied hostnames and usernames from the web interface to the SSH client without validation or sanitization. An attacker with network access to the Cockpit web service can craft a single HTTP request to the login end

9.9 **CVE-2026-23696** DETECTION

Windmill CE and EE versions 1.276.0 through 1.603.2 contain an SQL injection vulnerability in the folder ownership management functionality that allows authenticated attackers to inject SQL through the owner parameter. An attacker can use the injection to read

9.8 **CVE-2026-33439** Openidentityplatform openam DETECTION

Open Access Management (OpenAM) is an access management solution. Prior to 16.0.6, OpenIdentityPlatform OpenAM is vulnerable to pre-authentication Remote Code Execution (RCE) via unsafe Java deserialization of the jato.clientSession HTTP parameter. This bypass

9.8 **CVE-2021-4473** Topsecgroup tianxin internet behavior management system

Tianxin Internet Behavior Management System contains a command injection vulnerability in the Reporter component endpoint that allows unauthenticated attackers to execute arbitrary commands by supplying a crafted objClass parameter containing shell metacharact

9.8 **CVE-2024-36057**

Koha Library before 23.05.10 fails to sanitize user-controllable filenames prior to unzipping, leading to remote code execution. The line "qx/unzip $filename -d $dirname/;" in upload-cover-image.pl is vulnerable to command injection via shell metacharacters be

10.0 **CVE-2026-34078** Flatpak flatpak

Flatpak is a Linux application sandboxing and distribution framework. Prior to 1.16.4, the Flatpak portal accepts paths in the sandbox-expose options which can be app-controlled symlinks pointing at arbitrary paths. Flatpak run mounts the resolved host path in

9.8 **CVE-2026-21413** LibRaw LibRaw

Product not on watchlist.

9.1 **CVE-2026-39339** Churchcrm churchcrm DETECTION

ChurchCRM is an open-source church management system. Prior to 7.1.0, a critical authentication bypass vulnerability in ChurchCRM's API middleware (ChurchCRM/Slim/Middleware/AuthMiddleware.php) allows unauthenticated attackers to access all protected API endpo

9.8 **CVE-2026-20889** Libraw libraw

A heap-based buffer overflow vulnerability exists in the x3f_thumb_loader functionality of LibRaw Commit d20315b. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.

9.1 **CVE-2026-35573** Churchcrm churchcrm

ChurchCRM is an open-source church management system. Prior to 6.5.3, a path traversal vulnerability in ChurchCRM's backup restore functionality allows authenticated administrators to upload arbitrary files and achieve remote code execution by overwriting Apac

10.0 **CVE-2026-39337** Churchcrm churchcrm

ChurchCRM is an open-source church management system. Prior to 7.1.0, critical pre-authentication remote code execution vulnerability in ChurchCRM's setup wizard allows unauthenticated attackers to inject arbitrary PHP code during the initial installation proc

9.8 **CVE-2026-20911** Libraw libraw

A heap-based buffer overflow vulnerability exists in the HuffTable::initval functionality of LibRaw Commit 0b56545 and Commit d20315b. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger th

9.8 **CVE-2026-33815** Jackc pgx

+1 more CVEs in the same release

Memory-safety vulnerability in github.com/jackc/pgx/v5.

24 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. 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.