Daily brief, Wednesday, April 29, 2026

Apr 28, 8:00 PM to Apr 29, 8:00 PM ET

Generated Nov 7, 2026, 4:34 AM ET

0	0	0	13	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

13 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

13

9.0 **CVE-2026-42523** Jenkins github

Jenkins GitHub Plugin 1.46.0 and earlier improperly processes the current job URL as part of JavaScript implementing validation of the feature "GitHub hook trigger for GITScm polling", resulting in a stored cross-site scripting (XSS) vulnerability exploitable

10.0 **CVE-2026-3325** CRM Sistemas de Fidelización MegaCMS

SQL injection (SQLi) in MegaCMS v12.0.0, specifically in the “id_territorio” parameter of the “/web_comunications/cms/get_provincias” endpoint. The vulnerability arises from inadequate validation and sanitisation of user input. Specifically, via a POST request

9.8 **CVE-2026-42248** Ollama ollama

Ollama for Windows does not perform integrity or authenticity verification of downloaded update executables. Unlike other platforms, the Windows implementation of the update verification routine unconditionally returns success so no digital signature or trust

9.8 **CVE-2026-42249** Ollama ollama

Ollama for Windows contains a Remote Code Execution vulnerability in its update mechanism due to improper handling of attacker?controlled HTTP response headers. When downloading updates, the application constructs local file paths using values derived from HTT

9.8 **CVE-2026-36841**

TOTOLINK N200RE V5 was discovered to contain a command injection vulnerability via the macstr and bandstr parameters in the formMapDelDevice function.

9.8 **CVE-2026-38992**

Cockpit v2.13.5 and earlier is vulnerable to arbitrary code execution via the filter parameter within multiple endpoints. This vulnerability allows an attacker to run system commands on the underlying infrastructure via the MongoLite $func operator.

9.8 **CVE-2026-26015** Arc53 docsgpt

DocsGPT is a GPT-powered chat for documentation. From version 0.15.0 to before version 0.16.0, an attacker accessing both the official DocsGPT website or any local and public deployment, can craft a malicious payload bypassing the "MCP test" behavior to achiev

9.8 **CVE-2018-25316** Tenda w308r firmware

Tenda W308R v2 V5.07.48 contains a cookie session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient session validation. Attackers can send GET requests to the goform/AdvSetDns endpoint with a crafted

9.8 **CVE-2018-25317** Tenda w309r firmware

Tenda W3002R/A302/W309R wireless routers version V5.07.64_en contain a cookie session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient session validation. Attackers can send GET requests to the /gof

9.8 **CVE-2018-25318** Tenda fh303 firmware

Tenda FH303/A300 firmware V5.07.68_EN contains a session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient cookie validation. Attackers can send GET requests to the /goform/AdvSetDns endpoint with a

9.6 **CVE-2026-5166**

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Software Center allows Path Traversal. This issue affects Pardus Software Center: before 0.6.4.

9.1 **CVE-2026-7381** Miyagawa plack\

Plack::Middleware::XSendfile versions through 1.0053 for Perl can allow client-controlled path rewriting. Plack::Middleware::XSendfile allows the variation setting (sendfile type) to be set by the client via the X-Sendfile-Type header, if it is not considered

9.0 **CVE-2026-30893** Wazuh wazuh

Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 4.4.0 to before version 4.14.4, a path traversal vulnerability in Wazuh's cluster synchronization extraction routine allows an authenticated cluster peer

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.