Daily brief, Thursday, May 14, 2026

May 13, 8:00 PM to May 14, 8:00 PM ET

Generated Nov 7, 2026, 1:34 AM ET

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

1 newly exploited, 27 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2026-20182** Cisco Catalyst SD-WAN CISA KEV

Unauthenticated remote attacker can bypass authentication and gain administrative privileges on Cisco Catalyst SD-WAN Controller and Manager systems.

New public exploit code

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

New critical CVEs

27

10.0 **CVE-2026-20182** Cisco Catalyst SD-WAN KEV EXPLOIT CODE

Unauthenticated remote attacker can bypass authentication and gain administrative privileges on Cisco Catalyst SD-WAN Controller and Manager systems.

9.8 **CVE-2026-42589** Gotenberg gotenberg EXPLOIT CODE DETECTION

Product not on watchlist.

9.6 **CVE-2026-8511** Google chrome

Use after free in UI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-8580** Google chrome

Use after free in Mojo in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

10.0 **CVE-2026-44523**

Note Mark is an open-source note-taking application. Prior to 0.19.4, no minimum length or entropy is enforced on the JWT_SECRET configuration value. The application accepts any base64-decodable secret regardless of size, including secrets as short as 1 byte.

9.8 **CVE-2026-8181** DETECTION

The Burst Statistics – Privacy-Friendly WordPress Analytics (Google Analytics Alternative) plugin for WordPress is vulnerable to Authentication Bypass in versions 3.4.0 to 3.4.1.1. This is due to incorrect return-value handling in the `is_mainwp_authenticated(

9.8 **CVE-2026-6271**

The Career Section plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.7 via the CV upload handler. This is due to missing file type validation. This makes it possible for unauthenticated attackers to upload file

9.8 **CVE-2026-6510**

The InfusedWoo Pro plugin for WordPress is vulnerable to privilege escalation via missing authorization in all versions up to, and including, 5.1.2. This is due to missing nonce verification and capability checks in the iwar_save_recipe() AJAX handler. This ma

9.8 **CVE-2025-11024**

Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Akilli Commerce Software Technologies Ltd. Co. E-Commerce Website allows Blind SQL Injection. This issue affects E-Commerce Website: before 4.5.001.

9.8 **CVE-2026-2347**

Authorization bypass through User-Controlled key vulnerability in Akilli Commerce Software Technologies Ltd. Co. E-Commerce Website allows Session Hijacking. This issue affects E-Commerce Website: before 4.5.001.

9.8 **CVE-2026-44484** Lightningai pytorch lightning

PyTorch Lightning is a deep learning framework to pretrain and finetune AI models. Versions 2.6.2 and 2.6.2 have introduced functionality consistent with a credential harvesting mechanism.

9.8 **CVE-2026-41315** Midoks mdserver-web

mdserver-web is a simple Linux panel. From 0.18.0 to 0.18.4, mdserver-web has a front-end unauthorized remote command execution vulnerability. Due to the lack of authentication on the /modify_crond and /start_task interfaces, it is possible to modify the defau

9.8 **CVE-2026-26191** Fleetdm fleet

Fleet is open source device management software. Prior to version 4.81.0, a vulnerability in Fleet's software installer pipeline could allow a crafted software package to execute arbitrary commands as root (macOS/Linux) or SYSTEM (Windows) on managed endpoints

9.6 **CVE-2026-44482**

soundcloud-rpc is a SoundCloud Client with Discord Rich Presence, Dark Mode, Last.fm and AdBlock support. Prior to 0.1.8, a track title containing an HTML payload executed locally in the Electron app. This means attacker-controlled SoundCloud track metadata ca

9.6 **CVE-2026-41615** Microsoft authenticator

Exposure of sensitive information to an unauthorized actor in Microsoft Authenticator allows an unauthorized attacker to disclose information over a network.

9.4 **CVE-2026-42596** Thecodingmachine gotenberg DETECTION

Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.31.0, the default deny-lists used by Gotenberg's downloadFrom feature and webhook feature are bypassable. Because the filter is regex-based and case-sensitive, an unauthenticated attacker ca

9.4 **CVE-2026-44588**

SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, he tooltip mouseover handler in app/src/block/popover.ts reads aria-label via getAttribute and passes it through decodeURIComponent before assigning to messageElement.innerHTML in a

9.4 **CVE-2026-44592**

Gradient is a nix-based continuous integration system. In 1.1.0, when GRADIENT_DISCOVERABLE=true (the default, and the NixOS module default), anyone who can reach /proto can register as a worker without any credentials by sending a fresh, never-registered work

9.4 **CVE-2026-44670**

SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, the kernel stores Attribute View (AV / database) names without any HTML escape, then a render template uses raw strings.ReplaceAll(tpl, "${avName}", nodeAvName) to embed the name in

9.3 **CVE-2026-44212**

PrestaShop is an open source e-commerce web application. Prior to 8.2.6 and 9.1.1, there is a stored Cross-Site Scripting (XSS) vulnerability in the PrestaShop back-office Customer Service view. An unauthenticated attacker can submit the public Contact Us form

7 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Abrigo abrigo.com FINANCE 711,099 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.