Daily brief, Friday, May 15, 2026

May 14, 8:00 PM to May 15, 8:00 PM ET

Generated Nov 7, 2026, 1:20 AM ET

0	1	0	15	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 15 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.1 **CVE-2026-42897** Microsoft Microsoft CISA KEV DETECTION

Cross-site scripting in the Microsoft Exchange Server web interface lets an attacker access sensitive information and execute arbitrary code.

New public exploit code

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

New critical CVEs

15

10.0 **CVE-2026-41553** Dhtmlx pdf export module

PDF Export Module used in DHTMLX's products Gantt and Scheduler is vulnerable to Remote Code Execution due to lack of "data" parameter sanitization. An unauthenticated attacker can inject the malicious JavaScript code to the parameter whose value is processed

10.0 **CVE-2026-2031**

An Improper Access Control vulnerability in several internal API endpoints for Google Cloud Application Integration prior to 2026-01-23 allows a remote, unauthenticated attacker to disclose sensitive internal information and execute arbitrary code using specia

9.9 **CVE-2026-44774** Traefik traefik

Traefik is an HTTP reverse proxy and load balancer. Prior to 2.11.46, 3.6.17, and 3.7.1, Traefik's Kubernetes Gateway API provider allows a tenant with HTTPRoute creation permissions to expose the REST provider handler, bypassing the providers.rest.insecure=fa

9.8 **CVE-2026-5229**

The Form Notify plugin for WordPress is vulnerable to Authentication Bypass in versions up to and including 1.1.10. This is due to the plugin trusting user-controlled cookie data to determine which WordPress account to authenticate after a LINE OAuth login. Wh

9.8 **CVE-2026-45772** Vercel turborepo

Turborepo is a high-performance build system for JavaScript and TypeScript codebases. From 1.1.0 to before 2.9.14, Turborepo can be vulnerable to arbitrary code execution when run in untrusted repositories that contain malicious Yarn configuration. In affected

9.8 **CVE-2026-44717**

MCP Calculate Server is a mathematical calculation service based on MCP protocol and SymPy library. Prior to 0.1.1, the use of eval() to evaluate mathematical expressions without proper input sanitization leads to remote code execution. This vulnerability is f

9.8 **CVE-2021-47965**

WordPress Plugin WP Super Edit 2.5.4 and earlier contains an unrestricted file upload vulnerability in the FCKeditor component that allows attackers to upload dangerous file types without validation. Attackers can upload arbitrary files through the filemanager

9.8 **CVE-2026-46364** DETECTION

phpMyFAQ before 4.1.2 contains an unauthenticated SQL injection vulnerability in BuiltinCaptcha::garbageCollector() and BuiltinCaptcha::saveCaptcha() methods that interpolate unsanitized User-Agent headers into DELETE and INSERT queries. Unauthenticated attack

9.3 **CVE-2026-42155**

Magento Long Term Support (LTS) is an unofficial, community-driven project provides an alternative to the Magento Community Edition e-commerce platform with a high level of backward compatibility. Prior to 20.18.0, the XML-RPC / SOAP API session ID is generate

9.2 **CVE-2026-0481**

Unrestricted IP address binding in the AMD Device Metrics Exporter (ROCm ecosystem) could allow a remote attacker to perform unauthorized changes to the GPU configuration, potentially resulting in loss of availability

9.2 **CVE-2026-7182**

Diagram's export module is vulnerable to Path Traversal in src attribute due to lack of HTML sanitization. An unauthenticated user could craft the html payload which could include local files from the server and display them in the generated pdf. This issue wa

9.1 **CVE-2026-41258**

OpenMRS is an open source electronic medical record system platform. From 2.7.0 to before 2.7.9 and 2.8.6, the ConceptReferenceRangeUtility.evaluateCriteria() method in OpenMRS Core evaluates database-stored criteria strings as Apache Velocity templates withou

9.1 **CVE-2026-44699**

LibJWT is a C JSON Web Token Library. From 3.0.0 to 3.3.2, libjwt accepts an RSA JWK that does not contain an alg parameter as the verification key for an HS256/HS384/HS512 token. In the OpenSSL backend, this causes HMAC verification to run with a zero-length

9.1 **CVE-2026-45010**

phpMyFAQ before 4.1.2 contains an improper restriction of excessive authentication attempts vulnerability in the /admin/check endpoint, which accepts arbitrary user-id parameters without session binding or rate limiting. Unauthenticated attackers can brute-for

9.1 **CVE-2026-44551** Openwebui open webui DETECTION

Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the LDAP authentication endpoint does not validate that the submitted password is non-empty before performing a Simple Bind against the LDAP serv

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.