Daily brief, Monday, May 11, 2026

May 10, 8:00 PM to May 11, 8:00 PM ET

Generated Nov 7, 2026, 2:10 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

10.0 **CVE-2026-44643** Peerigon angular-expressions

Angular Expressions provides expressions for the Angular.JS web framework as a standalone module. Prior to 1.5.2, an attacker can write a malicious expression using filters that escapes the sandbox to execute arbitrary code on the system. This vulnerability is

10.0 **CVE-2026-42869**

SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.57, SOCFortress CoPilot ships a hardcoded JWT signing secret as a fallback value in backend/app/auth/utils.py:28 and ships it verbatim in .env.

9.9 **CVE-2026-7813** Pgadmin pgadmin 4

Authorization vulnerability in pgAdmin 4 server mode affecting Server Groups, Servers, Shared Servers, Background Processes, and Debugger modules. Multiple endpoints fetched user-owned objects without filtering by the requesting user's identity. An authenticat

9.9 **CVE-2026-42864**

FireFighter is an incident management application. Prior to 0.0.54, the POST /api/v2/firefighter/raid/jira_bot endpoint (CreateJiraBotView) is reachable without authentication (permission_classes = [permissions.AllowAny]). Its attachments payload is fetched se

9.8 **CVE-2026-40636** Dell elastic cloud storage

Dell ECS versions 3.8.1.0 through 3.8.1.7 and Dell ObjectScale versions prior to 4.3.0.0, contains a use of hard-coded credentials vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to filesystem

9.8 **CVE-2026-38567**

HireFlow v1.2 is vulnerable to SQL injection in the /login and /search endpoints. User-supplied input is concatenated directly into SQL queries without parameterization. An unauthenticated attacker can bypass authentication by supplying a crafted username (e.g

9.8 **CVE-2026-43995** Flowiseai flowise

Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, multiple tool implementations directly import and invoke raw HTTP clients (node-fetch, axios) instead of using the secured wrapper. These tools include (1)

9.6 **CVE-2026-43899**

+1 more CVEs in the same release

DeepChat is an open-source artificial intelligence agent platform that unifies models, tools, and agents. Prior to v1.0.4-beta.1, An incomplete mitigation for CVE-2025-55733 leaves DeepChat vulnerable to an arbitrary protocol execution bypass (RCE). While the

9.4 **CVE-2026-42613**

Grav is a file-based Web platform. Prior to 2.0.0-beta.2, the Login::register() method in the Login plugin accepts attacker-controlled groups and access fields from the registration POST data without server-side validation. When registration is enabled and gro

9.4 **CVE-2026-42882**

oxyno-zeta/s3-proxy is an aws s3 proxy written in go. Prior to 5.0.0, s3-proxy contains an authentication bypass caused by inconsistent URL path interpretation between the authentication middleware and the bucket handler. The authentication middleware evaluate

9.1 **CVE-2026-42607**

Grav is a file-based Web platform. Prior to 2.0.0-beta.2, an authenticated user with administrative privileges can achieve Remote Code Execution (RCE) by uploading a specially crafted ZIP file through the "Direct Install" tool. While the system attempts to blo

9.1 **CVE-2026-42608** Getgrav grav

Grav is a file-based Web platform. Prior to 2.0.0-beta.2, there is a Path Traversal vulnerability within the FormFlash core component. By manipulating the session_id (passed as __form-flash-id in POST requests), an unauthenticated attacker can traverse the fil

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.