Daily brief, Friday, May 29, 2026

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

Generated Nov 6, 2026, 3:22 PM ET

0	1	0	45	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 45 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

7.8 **CVE-2026-0257** Palo Alto Networks PAN-OS CISA KEV DETECTION

An authentication bypass in Palo Alto Networks PAN-OS before 10.2.5 gives attackers unauthorized access to the device and its network resources.

New public exploit code

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

New critical CVEs

45

10.0 **CVE-2026-8326**

Path traversal vulnerability in Remote Spark (https://www.Remotespark.Com/) SparkView allows reading and writing arbitrary files in all directories as root. This leads to RCE. The affected component is the RDP drive redirection. Depending on implementation, th

10.0 **CVE-2026-9508**

Incorrect permission settings on a critical resource in Suprema BioStar 2 (versions 2.9.3 through 2.9.11) that allow backup files to be publicly exposed when the administrator configures their path within the NGINX webroot. This vulnerability allows an attacke

10.0 **CVE-2026-45631**

Dokploy is a free, self-hostable Platform as a Service (PaaS). From 0.27.0 to before 0.29.3, a hardcoded BETTER_AUTH_SECRET fallback ("better-auth-secret-123456789") lets an unauthenticated attacker forge email verification JWTs, trigger auto-sign-in as admin,

9.9 **CVE-2026-9558**

A Server-Side Template Injection (SSTI) vulnerability exists in Mautic's theme engine. The platform renders uploaded Twig templates without a sandbox or strict function restrictions. Authenticated users with permissions to create or upload themes can abuse thi

9.9 **CVE-2026-9559**

A path traversal vulnerability exists in the campaign import feature of Mautic 7. When extracting uploaded ZIP files during campaign imports, a flaw in the validation logic allows file paths to escape the intended temporary directories. An authenticated user w

9.9 **CVE-2026-45312**

RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In 0.24.0 and earlier, a Jinja2 template injection in the prompt generator (rag/prompts/generator.py) allows any authenticated user to execute arbitrary OS commands on the server. Any norma

9.9 **CVE-2026-44962**

Plesk contains an XPath injection vulnerability in the APS Application Catalog search functionality, where user-supplied input is interpolated into XPath queries without proper sanitization. This allows an authenticated, low-privileged user to execute arbitrar

9.9 **CVE-2026-45663**

Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.29.1 and earlier, a command injection vulnerability exists in the Docker file upload functionality. When an authenticated user uploads a file to a container, the destinationPath parameter is n

9.9 **CVE-2026-45625**

Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to 1.19.0, Arcane's huma-based REST API exposes nine endpoints under /api/customize/git-repositories and /api/git-repositories/sync for managing GitOps source repositor

9.9 **CVE-2026-45629**

+1 more CVEs in the same release

Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.28.8 and earlier, authenticated OS command injection in the /listen-deployment WebSocket endpoint allows any organization member to execute arbitrary system commands on remote servers managed

9.9 **CVE-2026-45632**

Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.26.7 and earlier, the schedule router does not enforce organization/role checks. As a result, any authenticated user can create, update, run, or delete schedules belonging to other organizatio

9.9 **CVE-2026-45633**

Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.26.6 and earlier, Dokploy contains a command injection vulnerability in the /docker-container-logs WebSocket endpoint. The tail and since parameters are not validated and are directly concaten

9.9 **CVE-2026-45661**

Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.26.5 and earlier, a critical path traversal vulnerability exists in Dokploy v0.26.5 that allows authenticated users to write arbitrary files to the filesystem during application deployment. Wh

9.9 **CVE-2026-47744**

Shopper is a Headless e-commerce Admin Panel. Prior to 2.8.0, two distinct authorization defects in the team settings allowed any authenticated panel user to take over the RBAC system. Settings/Team/Index had no mount() authorization. Any authenticated user co

9.9 **CVE-2026-45372** Yhirose cpp-httplib

cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.44.0, when cpp-httplib's server parses an incoming request, it applies percent-decoding to every header value except Location and Referer. The validity check (is_field

9.8 **CVE-2026-8732** DETECTION

The WP Maps Pro plugin for WordPress is vulnerable to Privilege Escalation via Administrator Account Creation in all versions up to, and including, 6.1.0. This is due to the wpgmp_temp_access_ajax AJAX action being registered with wp_ajax_nopriv_ and protected

9.8 **CVE-2026-3655**

The OTP Login With Phone Number, OTP Verification plugin for WordPress is vulnerable to authentication bypass in versions 1.8.50 through 1.8.60. This is due to the Firebase verification flow in the `lwp_ajax_register` AJAX handler not binding the Firebase sess

9.8 **CVE-2026-49197** Acer predator connect w6x firmware

Web endpoints intended for the Acer Connect app improperly validate the HTTP Authorization header, failing to block requests when Base64 decoding fails.

9.8 **CVE-2026-49199** Acer predator connect w6x firmware

Crafted MQTT messages can trigger command injection, resulting in root-level code execution on the target device.

9.8 **CVE-2026-49200** Acer wave 7 firmware

The acer_cgi.log file in the device firmware is accessible without authentication via the web interface. This file contains cleartext login credentials (for web and Telnet), leading to unauthorized system access.

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.