Daily brief, Wednesday, May 27, 2026

May 26, 8:00 PM to May 27, 8:00 PM ET

Generated Nov 6, 2026, 11:02 PM ET

0	3	0	47	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 47 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

9.8 **CVE-2026-8398** Daemon Daemon Tools Lite CISA KEV

Malicious code embedded in Daemon Tools Lite gives an attacker high impact on confidentiality, integrity, and availability.

9.6 **CVE-2026-45321** TanStack TanStack CISA KEV

Unspecified TanStack flaw lets attackers publish malicious TanStack versions to npm under a trusted identity, distributing credential-stealing malware.

9.3 **CVE-2026-48027** Nx Nx Console CISA KEV

A malicious published version of the Nx Console extension fetched an obfuscated payload that harvests credentials from disk and memory.

New public exploit code

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

New critical CVEs

47

9.6 **CVE-2026-45321** TanStack TanStack KEV EXPLOIT CODE

Unspecified TanStack flaw lets attackers publish malicious TanStack versions to npm under a trusted identity, distributing credential-stealing malware.

9.3 **CVE-2026-48027** Nx Nx Console KEV

A malicious published version of the Nx Console extension fetched an obfuscated payload that harvests credentials from disk and memory.

9.8 **CVE-2026-8398** Daemon Daemon Tools Lite KEV

Malicious code embedded in Daemon Tools Lite gives an attacker high impact on confidentiality, integrity, and availability.

10.0 **CVE-2026-8054** dotCMS dotCMS Core EXPLOIT CODE DETECTION

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in the Publish Audit API endpoints (/api/auditPublishing/get and /api/auditPublishing/getAll) in dotCMS Core 25.11.04-1 through 26.04.28-02 allows remote unauthenticated attac

9.8 **CVE-2026-45898** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: RDMA/iwcm: Fix workqueue list corruption by removing work_list The commit e1168f0 ("RDMA/iwcm: Simplify cm_event_handler()") changed the work submission logic to unconditionally call queue_wor

9.8 **CVE-2026-45972** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF and double free in smb2_open_file() Zero out @err_iov and @err_buftype before retrying SMB2_open() to prevent an UAF bug if @data != NULL, otherwise a double fre

9.8 **CVE-2026-45988** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix re-decryption of RESPONSE packets If a RESPONSE packet gets a temporary failure during processing, it may end up in a partially decrypted state - and then get requeued for a retry.

9.8 **CVE-2026-46039** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: rxgk: Fix potential integer overflow in length check Fix potential integer overflow in rxgk_extract_token() when checking the length of the ticket. Rather than rounding up the value to be test

9.1 **CVE-2026-46043** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Validate pad and ICRC before payload_size() in rxe_rcv rxe_rcv() currently checks only that the incoming packet is at least header_size(pkt) bytes long before payload_size() is used.

9.8 **CVE-2025-12686** Synology BeeStation OS

Product not on watchlist.

9.8 **CVE-2026-45083** Intranda goobi-viewer-core

The Goobi viewer is a web application that allows digitised material to be displayed in a web browser. From 4.8.0 to before 26.04.1, the Goobi viewer REST endpoint POST /api/v1/index/stream accepted an arbitrary Solr streaming expression from unauthenticated n

9.8 **CVE-2026-42731** miniOrange miniorange otp verification

Incorrect Privilege Assignment vulnerability in miniOrange miniorange otp verification miniorange-otp-verification allows Privilege Escalation.This issue affects miniorange otp verification: from n/a through <= 5.4.9.

9.3 **CVE-2026-42727** RealMag777 Active Products Tables for WooCommerce

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 Active Products Tables for WooCommerce profit-products-tables-for-woocommerce allows Blind SQL Injection.This issue affects Active Products Tables

9.4 **CVE-2026-9739** Google MCP Toolbox for Databases

Vulnerable to DNS rebinding attacks when using SSE (http://b/499408790). During the beta phase, we implemented `allowed-origins` and `allowed-hosts` flags to align with MCP security guidelines. However, the hardcoded `Access-Control-Allow-Origin: *` header in

10.0 **CVE-2026-44327** Free5gc free5gc

free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF mounts the nnef-oam route group without inbound OAuth2/bearer-token authorization. A network attacker who can reach NEF on the SBI can hit the OAM route with no Auth

10.0 **CVE-2026-44329** Free5gc free5gc

free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's SMF mounts the UPI management route group without OAuth2/bearer-token authorization middleware. A network attacker who can reach SMF on the SBI can hit UPI endpoints wit

10.0 **CVE-2026-44330** Free5gc free5gc

free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2, free5GC's NEF mounts the nnef-pfdmanagement route group without inbound OAuth2/bearer-token authorization. A network attacker who can reach NEF on the SBI can use a forged or arbi

10.0 **CVE-2026-45087**

Dalfox is a powerful open-source XSS scanner and utility focused on automation. Prior to 2.13.0, when dalfox is started in REST API server mode (dalfox server), the server binds to 0.0.0.0:6664 by default and requires no API key unless the operator explicitly

9.9 **CVE-2026-42748**

Unrestricted Upload of File with Dangerous Type vulnerability in WPify WPify Woo Czech wpify-woo allows Upload a Web Shell to a Web Server.This issue affects WPify Woo Czech: from n/a through <= 5.4.1.

9.9 **CVE-2026-42756**

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ludwig You QuickWebP – Compress / Optimize Images & Convert WebP | SEO Friendly quickwebp allows Path Traversal.This issue affects QuickWebP – Compr

27 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Mytheresa mytheresa.com 84,108 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.