Daily brief, Thursday, May 21, 2026

May 20, 8:00 PM to May 21, 8:00 PM ET

Generated Nov 7, 2026, 12:08 AM ET

0	2	0	12	0	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 12 new critical CVEs, 2 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

9.4 **CVE-2025-34291** Langflow Langflow CISA KEV DETECTION

Langflow's permissive CORS and SameSite=None refresh cookie let a malicious webpage make credentialed cross-origin calls to the token refresh endpoint.

6.7 **CVE-2026-34926** Trend Micro Apex One CISA KEV

Trend Micro Apex One on-premise directory traversal lets a pre-authenticated local attacker alter a server key table to push malicious code to agents.

New public exploit code

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

New critical CVEs

12

9.4 **CVE-2025-34291** Langflow Langflow KEV EXPLOIT CODE DETECTION

Langflow's permissive CORS and SameSite=None refresh cookie let a malicious webpage make credentialed cross-origin calls to the token refresh endpoint.

9.8 **CVE-2026-43501** Linux Linux EXPLOIT CODE

In the Linux kernel, the following vulnerability has been resolved: ipv6: rpl: reserve mac_len headroom when recompressed SRH grows ipv6_rpl_srh_rcv() decompresses an RFC 6554 Source Routing Header, swaps the next segment into ipv6_hdr->daddr, recompresses, th

10.0 **CVE-2026-9152**

A missing authentication vulnerability exists in the Altium 365 SearchService. A legacy SOAP endpoint exposes search index operations without requiring authentication, session tokens, or any form of identity verification. An unauthenticated network attacker wh

9.9 **CVE-2026-44050**

A heap-based buffer overflow in the CNID daemon comm_rcv() function in Netatalk 2.0.0 through 4.4.2 allows a remote authenticated attacker to execute arbitrary code with escalated privileges or cause a denial of service.

9.8 **CVE-2026-6279** DETECTION

The Avada Builder (fusion-builder) plugin for WordPress is vulnerable to Unauthenticated Remote Code Execution via PHP Function Injection in versions up to and including 3.15.2. This is due to the `wp_conditional_tags` case in `Fusion_Builder_Conditional_Rende

9.8 **CVE-2026-5118**

The Divi Form Builder plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.1.2. This is due to the plugin accepting a user-controlled 'role' parameter from POST data during user registration without validating it again

9.8 **CVE-2025-71210** Trendmicro apex one

+1 more CVEs in the same release

A vulnerability in the Trend Micro Apex One management console could allow a remote attacker to upload malicious code and execute commands on affected installations. Please note: although this vulnerability carries a technical critical CVSS rating, this was re

9.8 **CVE-2026-48207** Apache fory

Deserialization of untrusted data in Apache Fory PyFory. PyFory's ReduceSerializer could bypass documented DeserializationPolicy validation hooks during reduce-state restoration and global-name resolution. An application is vulnerable if it deserializes attack

9.8 **CVE-2026-6960**

The BookingPress Pro plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'bookingpress_validate_submitted_booking_form_func' function in all versions up to, and including, 5.6. This makes it possible for unau

9.3 **CVE-2026-39531**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wp Directory Kit WP Directory Kit allows Blind SQL Injection. This issue affects WP Directory Kit: from n/a through 1.5.0.

9.1 **CVE-2026-5433**

Honeywell Control Network Module (CNM) contains command injection vulnerability in the web interface. An attacker could exploit this vulnerability via command delimiters, potentially resulting in Remote Code Execution (RCE). Honeywell recommends updating to th

Ransomware

No leak-site posts collected.

New data breaches 2

Dragonica Lunaris	playdragonica.eu	126,293 accounts
Windows93 / Myspace93	windows93.net	46,105 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.