Daily brief, Friday, May 1, 2026

Apr 30, 8:00 PM to May 1, 8:00 PM ET

Generated Nov 7, 2026, 4:14 AM ET

0	1	0	22	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 22 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

7.8 **CVE-2026-31431** Linux Kernel CISA KEV DETECTION

An attacker gains arbitrary read and write access to kernel memory in the Linux kernel memory management subsystem.

New public exploit code

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

New critical CVEs

22

9.8 **CVE-2026-31705** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix out-of-bounds write in smb2_get_ea() EA alignment smb2_get_ea() applies 4-byte alignment padding via memset() after writing each EA entry. The bounds check on buf_free_len is perfor

9.8 **CVE-2026-31718** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in __ksmbd_close_fd() via durable scavenger When a durable file handle survives session disconnect (TCP close without SMB2_LOGOFF), session_fd_check() sets fp->conn =

9.8 **CVE-2026-43011** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net/x25: Fix potential double free of skb When alloc_skb fails in x25_queue_rx_frame it calls kfree_skb(skb) at line 48 and returns 1 (error). This error propagates back through the call chain

9.8 **CVE-2026-43037** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ip6_tunnel: clear skb2->cb[] in ip4ip6_err() Oskar Kjos reported the following problem. ip4ip6_err() calls icmp_send() on a cloned skb whose cb[] was written by the IPv6 receive path as struct

9.8 **CVE-2026-43038** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ipv6: icmp: clear skb2->cb[] in ip6_err_gen_icmpv6_unreach() Sashiko AI-review observed: In ip6_err_gen_icmpv6_unreach(), the skb is an outer IPv4 ICMP error packet where its cb contains an IP

9.8 **CVE-2026-43039** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: ti: icssg-prueth: fix missing data copy and wrong recycle in ZC RX dispatch emac_dispatch_skb_zc() allocates a new skb via napi_alloc_skb() but never copies the packet data from the XDP b

9.8 **CVE-2026-37531** Linuxfoundation automotive grade linux

AGL app-framework-main thru 17.1.12 contains a Zip Slip path traversal vulnerability (CWE-22) combined with a TOCTOU race condition (CWE-367) in the widget installation flow. The is_valid_filename function in wgtpkg-zip.c validates ZIP entry names but does not

10.0 **CVE-2026-42996**

JS8Call through 2.3.1 and JS8Call-improved before 3.0 have a stack-based buffer overflow via a radio transmission of @APRSIS GRID followed by a long Maidenhead locator. This occurs in grid2deg in APRSISClient.cpp.

10.0 **CVE-2026-37541** Openvehicles open vehicle monitoring system firmware

Buffer overflow vulnerability in Open Vehicle Monitoring System 3 (OVMS3) 3.3.005. In canformat_gvret.cpp, the length field in GVRET binary data is not properly validated, allowing remote attackers to cause a denial of service or possibly execute arbitrary cod

9.8 **CVE-2026-7538**

A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function Vulnerability of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument proto leads to os command injection. The attac

9.8 **CVE-2026-7546**

A security vulnerability has been detected in Totolink NR1800X 9.1.0u.6279_B20210910. The impacted element is the function find_host_ip of the component lighttpd. Such manipulation of the argument Host leads to stack-based buffer overflow. The attack can be ex

9.8 **CVE-2026-42994** Bitwarden cli

Bitwarden CLI 2026.4.0 from 2026-04-22T21:57Z to 2026-04-22T23:30Z, when obtained from npm, had embedded malicious code. This is related to a Checkmarx supply chain incident.

9.8 **CVE-2026-7567**

The Temporary Login plugin for WordPress is vulnerable to Authentication Bypass in versions up to and including 1.0.0. This is due to improper input validation in the maybe_login_temporary_user() function, which fails to verify that the 'temp-login-token' GET

9.8 **CVE-2026-42778** Apache mina

The fix for CVE-2026-41409 was not applied to the 2.1.X and 2.2.X branches. Here was the original issue description: The fix for CVE-2024-52046 in Apache MINA AbstractIoBuffer.getObject() was incomplete. The classname allowlist of classes allowed to be deseria

9.8 **CVE-2026-42779** Apache mina

The fix for CVE-2026-41635 was not applied to the 2.1.X and 2.2.X branches. Here was the original issue description: Apache MINA's AbstractIoBuffer.resolveClass() contains two branches, one of them (for static classes or primitive types) does not check the cla

9.8 **CVE-2026-42482** Hashcat hashcat

A stack-based buffer overflow in mangle_to_hex_lower() and mangle_to_hex_upper() in src/rp_cpu.c in hashcat v7.1.2 allows an attacker to cause a denial of service or possibly execute arbitrary code via a crafted rule file, or via the -j or -k rule options used

9.8 **CVE-2026-42483** Hashcat hashcat

A heap-based buffer overflow in the Kerberos hash parser in hashcat v7.1.2 allows an attacker to cause a denial of service or possibly execute arbitrary code via a crafted Kerberos hash file. The issue affects module_hash_decode in multiple Kerberos-related mo

9.8 **CVE-2026-42484** Hashcat hashcat

A heap-based buffer overflow in hex_to_binary in the PKZIP hash parser in hashcat v7.1.2 allows an attacker to cause a denial of service or possibly execute arbitrary code via a crafted PKZIP hash file. The issue affects modules 17200, 17210, 17220, 17225, and

9.8 **CVE-2026-42472**

+1 more CVEs in the same release

Unsafe deserialization vulnerability in MixPHP Framework 2.x thru 2.2.17. The session and cache handlers use unserialize() on data from Redis in the RedisHandler object.

9.8 **CVE-2026-37534**

Integer underflow vulnerability in Open-SAE-J1939 thru commit b6caf884df46435e539b1ecbf92b6c29b345bdfe (2025-11-30) in SAE_J1939_Read_Transport_Protocol_Data_Transfer,allows attackers to write to arbitrary memory via crafted sequence number from the CAN frame.

1 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Aman aman.com 215,563 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.