Daily brief, Friday, April 3, 2026

Apr 2, 8:00 PM to Apr 3, 8:00 PM ET

Generated Nov 7, 2026, 9:21 AM ET

0	0	0	32	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

32 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

32

9.1 **CVE-2026-23455** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_h323: check for zero length in DecodeQ931() In DecodeQ931(), the UserUserIE code path reads a 16-bit length from the packet, then decrements it by 1 to skip the protoco

9.8 **CVE-2026-31402** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: nfsd: fix heap overflow in NFSv4.0 LOCK replay cache The NFSv4.0 replay cache uses a fixed 112-byte inline buffer (rp_ibuf[NFSD4_REPLAY_ISIZE]) to store encoded operation responses. This size

10.0 **CVE-2026-32213** Microsoft azure ai foundry

Improper authorization in Azure AI Foundry allows an unauthorized attacker to elevate privileges over a network.

9.1 **CVE-2026-32211** Microsoft azure web apps

Missing authentication for critical function in Azure MCP Server allows an unauthorized attacker to disclose information over a network.

10.0 **CVE-2026-33105** Microsoft azure kubernetes service

Improper authorization in Microsoft Azure Kubernetes Service allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-33107** Microsoft azure databricks

Server-side request forgery (ssrf) in Azure Databricks allows an unauthorized attacker to elevate privileges over a network.

9.6 **CVE-2026-26135** Microsoft azure custom locations resource provider

Server-side request forgery (ssrf) in Azure Custom Locations Resource Provider (RP) allows an authorized attacker to elevate privileges over a network.

9.8 **CVE-2026-23450** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net/smc: fix NULL dereference and UAF in smc_tcp_syn_recv_sock() Syzkaller reported a panic in smc_tcp_syn_recv_sock() [1]. smc_tcp_syn_recv_sock() is called in the TCP receive path (softirq)

9.8 **CVE-2026-23428** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free of share_conf in compound request smb2_get_ksmbd_tcon() reuses work->tcon in compound requests without validating tcon->t_state. ksmbd_tree_conn_lookup() checks t_sta

9.8 **CVE-2026-23427** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in durable v2 replay of active file handles parse_durable_handle_context() unconditionally assigns dh_info->fp->conn to the current connection when handling a DURABLE

10.0 **CVE-2026-34938** Praison praisonaiagents

PraisonAI is a multi-agent teams system. Prior to version 1.5.90, execute_code() in praisonai-agents runs attacker-controlled Python inside a three-layer sandbox that can be fully bypassed by passing a str subclass with an overridden startswith() method to the

9.0 **CVE-2026-35216** Budibase budibase

Budibase is an open-source low-code platform. Prior to version 3.33.4, an unauthenticated attacker can achieve Remote Code Execution (RCE) on the Budibase server by triggering an automation that contains a Bash step via the public webhook endpoint. No authenti

9.8 **CVE-2026-0545** Lfprojects mlflow DETECTION

In mlflow/mlflow, the FastAPI job endpoints under `/ajax-api/3.0/jobs/*` are not protected by authentication or authorization when the `basic-auth` app is enabled. This vulnerability affects the latest version of the repository. If job execution is enabled (`M

9.8 **CVE-2017-20237**

Hirschmann Industrial HiVision versions prior to 06.0.07 and 07.0.03 contains an authentication bypass vulnerability in the master service that allows unauthenticated remote attackers to execute arbitrary commands with administrative privileges. Attackers can

9.8 **CVE-2026-34935** Praison praisonai

PraisonAI is a multi-agent teams system. From version 4.5.15 to before version 4.5.69, the --mcp CLI argument is passed directly to shlex.split() and forwarded through the call chain to anyio.open_process() with no validation, allowlist check, or sanitization

9.8 **CVE-2018-25237**

Hirschmann HiSecOS devices versions prior to 05.3.03 contain a buffer overflow vulnerability in the HTTPS login interface when RADIUS authentication is enabled that allows remote attackers to crash the device or execute arbitrary code by submitting a password

10.0 **CVE-2026-32186** Microsoft bing

Server-side request forgery (ssrf) in Microsoft Bing allows an unauthorized attacker to elevate privileges over a network.

9.8 **CVE-2017-20236** Prosoft-Technology icx35-hwc firmware

ProSoft Technology ICX35-HWC versions 1.3 and prior cellular gateways contain an input validation vulnerability in the web user interface that allows remote attackers to inject and execute system commands by submitting malicious input through unvalidated field

9.9 **CVE-2026-34612** Kestra kestra

Kestra is an open-source, event-driven orchestration platform. Prior to version 1.3.7, Kestra (default docker-compose deployment) contains a SQL Injection vulnerability that leads to Remote Code Execution (RCE) in the following endpoint "GET /api/v1/main/flows

9.8 **CVE-2026-27634** Piwigo piwigo

Piwigo is an open source photo gallery application for the web. Prior to version 16.3.0, the four date filter parameters (f_min_date_available, f_max_date_available, f_min_date_created, f_max_date_created) in ws_std_image_sql_filter() are concatenated directly

12 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.