Daily brief, Tuesday, December 16, 2025

Dec 15, 7:00 PM to Dec 16, 7:00 PM ET

Generated Nov 9, 2026, 4:16 AM ET

0	1	0	25	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 25 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.1 **CVE-2025-59718** Fortinet Multiple Products CISA KEV

Attacker gains remote code execution and unauthorized access to sensitive data in Fortinet FortiGate, FortiManager, FortiAnalyzer, and FortiOS via improper signature verification.

New public exploit code

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

New critical CVEs

25

9.1 **CVE-2025-59718** Fortinet Multiple Products KEV EXPLOIT CODE

Attacker gains remote code execution and unauthorized access to sensitive data in Fortinet FortiGate, FortiManager, FortiAnalyzer, and FortiOS via improper signature verification.

9.8 **CVE-2023-53894** Dulldusk phpfilemanager

phpfm 1.7.9 contains an authentication bypass vulnerability that allows attackers to log in by exploiting loose type comparison in password hash validation. Attackers can craft specific password hashes beginning with 0e or 00e to bypass authentication and uplo

10.0 **CVE-2025-63414** Allskyteam allsky

A Path Traversal vulnerability in the Allsky WebUI version v2024.12.06_06 allows an unauthenticated remote attacker to achieve arbitrary command execution. By sending a crafted HTTP request to the /html/execute.php endpoint with a malicious payload in the id p

9.8 **CVE-2025-46295** Claris filemaker server

Apache Commons Text versions prior to 1.10.0 included interpolation features that could be abused when applications passed untrusted input into the text-substitution API. Because some interpolators could trigger actions like executing commands or accessing ext

9.8 **CVE-2025-62849** Qnap qts

An SQL injection vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to execute unauthorized code or commands. We have already fixed the vulnerability in the following versio

9.8 **CVE-2023-53895** Potsky pimp my log

PimpMyLog 1.7.14 contains an improper access control vulnerability that allows remote attackers to create admin accounts without authorization through the configuration endpoint. Attackers can exploit the unsanitized username field to inject malicious JavaScri

9.0 **CVE-2025-33210** Nvidia isaac lab

NVIDIA Isaac Lab contains a deserialization vulnerability. A successful exploit of this vulnerability might lead to code execution.

9.8 **CVE-2025-59385** Qnap qts

An authentication bypass by spoofing vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to access resources which are not otherwise accessible without proper authentication.

9.6 **CVE-2025-67744** Thinkinai deepchat

DeepChat is an open-source artificial intelligence agent platform that unifies models, tools, and agents. Prior to version 0.5.3, a security vulnerability exists in the Mermaid diagram rendering component that allows arbitrary JavaScript execution. Due to the

9.8 **CVE-2025-68192**

In the Linux kernel, the following vulnerability has been resolved: net: usb: qmi_wwan: initialize MAC header offset in qmimux_rx_fixup Raw IP packets have no MAC header, leaving skb->mac_header uninitialized. This can trigger kernel panics on ARM64 when xfrm

9.8 **CVE-2025-68284**

In the Linux kernel, the following vulnerability has been resolved: libceph: prevent potential out-of-bounds writes in handle_auth_session_key() The len field originates from untrusted network packets. Boundary checks have been added to prevent potential out-o

9.8 **CVE-2025-68285**

In the Linux kernel, the following vulnerability has been resolved: libceph: fix potential use-after-free in have_mon_and_osd_map() The wait loop in __ceph_open_session() can race with the client receiving a new monmap or osdmap shortly after the initial map i

9.8 **CVE-2023-53899** Podcastgenerator podcast generator

PodcastGenerator 3.2.9 contains a blind server-side request forgery vulnerability that allows attackers to inject XML in the episode upload form. Attackers can manipulate the 'shortdesc' parameter to trigger external HTTP requests to arbitrary endpoints during

9.1 **CVE-2025-65319** Blixhq bluemail

When using the attachment interaction functionality, Blue Mail 1.140.103 and below saves documents to a file system without a Mark-of-the-Web tag, which allows attackers to bypass the built-in file protection mechanisms of both Windows OS and third-party softw

9.1 **CVE-2025-65318** Canarymail canary mail

When using the attachment interaction functionality, Canary Mail 5.1.40 and below saves documents to a file system without a Mark-of-the-Web tag, which allows attackers to bypass the built-in file protection mechanisms of both Windows OS and third-party softwa

9.8 **CVE-2025-40350**

In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: RX, Fix generating skb from non-linear xdp_buff for striding RQ XDP programs can change the layout of an xdp_buff through bpf_xdp_adjust_tail() and bpf_xdp_adjust_head(). Therefore,

9.8 **CVE-2025-68301**

In the Linux kernel, the following vulnerability has been resolved: net: atlantic: fix fragment overflow handling in RX path The atlantic driver can receive packets with more than MAX_SKB_FRAGS (17) fragments when handling large multi-descriptor packets. This

9.8 **CVE-2025-68263**

In the Linux kernel, the following vulnerability has been resolved: ksmbd: ipc: fix use-after-free in ipc_msg_send_request ipc_msg_send_request() waits for a generic netlink reply using an ipc_msg_table_entry on the stack. The generic netlink handler (handle_g

9.8 **CVE-2025-68315**

In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to detect potential corrupted nid in free_nid_list As reported, on-disk footer.ino and footer.nid is the same and out-of-range, let's add sanity check on f2fs_alloc_nid() to detect a

9.8 **CVE-2025-50401** Mercurycom d196g firmware

+1 more CVEs in the same release

Mercury D196G d196gv1-cn-up_2020-01-09_11.21.44 is vulnerable to Buffer Overflow in the function sub_404CAEDC via the parameter password.

4 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.