Daily brief, Tuesday, December 23, 2025

Dec 22, 7:00 PM to Dec 23, 7:00 PM ET

Generated Nov 9, 2026, 3:04 AM ET

0	0	0	24	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

24 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

24

10.0 **CVE-2024-57521** Ruoyi ruoyi EXPLOIT CODE

SQL Injection vulnerability in RuoYi v.4.7.9 and before allows a remote attacker to execute arbitrary code via the createTable function in SqlUtil.java.

9.3 **CVE-2025-68664** Langchain langchain core

LangChain is a framework for building agents and LLM-powered applications. Prior to versions 0.3.81 and 1.2.5, a serialization injection vulnerability exists in LangChain's dumps() and dumpd() functions. The functions do not escape dictionaries with 'lc' keys

9.8 **CVE-2025-68615** Net-Snmp net-snmp

net-snmp is a SNMP application library, tools and daemon. Prior to versions 5.9.5 and 5.10.pre2, a specially crafted packet to an net-snmp snmptrapd daemon can cause a buffer overflow and the daemon to crash. This issue has been patched in versions 5.9.5 and 5

9.9 **CVE-2025-66209** Coollabs coolify

Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in the Database Backup functionality allows users with application/service man

9.8 **CVE-2025-14500** DETECTION

IceWarp14 X-File-Operation Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IceWarp. Authentication is not required to exploit this vulnerability. The speci

9.8 **CVE-2025-29229** Linksys e5600 firmware

linksys E5600 V1.1.0.26 is vulnerable to command injection in the function ddnsStatus.

9.8 **CVE-2025-29228** Linksys e5600 firmware

Linksys E5600 V1.1.0.26 is vulnerable to command injection in the runtime.macClone function via the mc.ip parameter.

10.0 **CVE-2025-14931**

Hugging Face smolagents Remote Python Executor Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face smolagents. Authentication is n

9.8 **CVE-2025-50526** Netgear ex8000 firmware

Netgear EX8000 V1.0.0.126 was discovered to contain a command injection vulnerability via the switch_status function.

9.8 **CVE-2025-15047** Tenda wh450 firmware

A vulnerability was found in Tenda WH450 1.0.0.18. This affects an unknown function of the file /goform/PPTPDClient of the component HTTP Request Handler. Performing a manipulation of the argument Username results in stack-based buffer overflow. The attack can

9.8 **CVE-2025-15044** Tenda wh450 firmware

A vulnerability was detected in Tenda WH450 1.0.0.18. Impacted is an unknown function of the file /goform/NatStaticSetting. The manipulation of the argument page results in stack-based buffer overflow. The attack may be performed from remote. The exploit is no

9.8 **CVE-2025-15045** Tenda wh450 firmware

A flaw has been found in Tenda WH450 1.0.0.18. The affected element is an unknown function of the file /goform/Natlimit of the component HTTP Request Handler. This manipulation of the argument page causes stack-based buffer overflow. It is possible to initiate

9.8 **CVE-2025-15046** Tenda wh450 firmware

A vulnerability has been found in Tenda WH450 1.0.0.18. The impacted element is an unknown function of the file /goform/PPTPClient of the component HTTP Request Handler. Such manipulation of the argument netmsk leads to stack-based buffer overflow. It is possi

9.8 **CVE-2025-33224** Nvidia isaac launchable

+1 more CVEs in the same release

NVIDIA Isaac Launchable contains a vulnerability where an attacker could cause an execution with unnecessary privileges. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosur

9.8 **CVE-2025-33222** Nvidia isaac launchable

NVIDIA Isaac Launchable contains a vulnerability where an attacker could exploit a hard-coded credential issue. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, and data tampering.

9.9 **CVE-2025-68667**

Conduit is a chat server powered by Matrix. A vulnerability that affects a number of Conduit-derived homeservers allows a remote, unauthenticated attacker to force the target server to cryptographically sign arbitrary membership events. Affected products inclu

9.8 **CVE-2025-65354** Puneethreddyhc event management

Improper input handling in /Grocery/search_products_itname.php inPuneethReddyHC event-management 1.0 permits SQL injection via the sitem_name POST parameter. Crafted payloads can alter query logic and disclose database contents. Exploitation may result in sens

9.8 **CVE-2025-14388**

The PhastPress plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Read via null byte injection in all versions up to, and including, 3.7. This is due to a discrepancy between the extension validation in `getExtensionForURL()` which operates o

9.6 **CVE-2025-68669** 5ire 5ire

5ire is a cross-platform desktop artificial intelligence assistant and model context protocol client. In versions 0.15.2 and prior, an RCE vulnerability exists in useMarkdown.ts, where the markdown-it-mermaid plugin is initialized with securityLevel: 'loose'.

9.8 **CVE-2025-68341**

In the Linux kernel, the following vulnerability has been resolved: veth: reduce XDP no_direct return section to fix race As explain in commit fa349e396e48 ("veth: Fix race with AF_XDP exposing old or uninitialized descriptors") for veth there is a chance afte

3 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.