Daily brief, Friday, January 23, 2026

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

Generated Nov 7, 2026, 9:03 PM ET

0	1	0	35	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 35 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2024-37079** Broadcom VMware vCenter Server CISA KEV

An out-of-bounds write in Broadcom VMware vCenter Server lets an attacker gain unauthorized access to sensitive data and compromise the system.

New public exploit code

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

New critical CVEs

35

9.8 **CVE-2024-37079** Broadcom VMware vCenter Server KEV

An out-of-bounds write in Broadcom VMware vCenter Server lets an attacker gain unauthorized access to sensitive data and compromise the system.

9.8 **CVE-2026-0769** Langflow Langflow EXPLOIT CODE

Product not on watchlist.

9.8 **CVE-2026-0768** Langflow Langflow EXPLOIT CODE DETECTION

Product not on watchlist.

9.9 **CVE-2026-24304** Microsoft azure resource manager

Improper access control in Azure Resource Manager allows an authorized attacker to elevate privileges over a network.

9.8 **CVE-2026-22984** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: libceph: prevent potential out-of-bounds reads in handle_auth_done() Perform an explicit bounds check on payload_len to avoid a possible out-of-bounds access in the callout. [idryomov: change

9.8 **CVE-2025-71159** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free warning in btrfs_get_or_create_delayed_node() Previously, btrfs_get_or_create_delayed_node() set the delayed_node's refcount before acquiring the root->delayed_nodes

9.8 **CVE-2022-25369** DETECTION

An issue was discovered in Dynamicweb before 9.12.8. An attacker can add a new administrator user without authentication. This flaw exists due to a logic issue when determining if the setup phases of the product can be run again. Once an attacker is authentica

9.8 **CVE-2026-0755**

gemini-mcp-tool execAsync Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of gemini-mcp-tool. Authentication is not required to exploit this vulnerability. Th

9.8 **CVE-2026-0761** Deepwisdom metagpt

Foundation Agents MetaGPT actionoutput_str_to_mapping Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foundation Agents MetaGPT. Authentication is not require

9.8 **CVE-2025-15061**

Framelink Figma MCP Server fetchWithRetry Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Framelink Figma MCP Server. Authentication is not required to exp

9.8 **CVE-2025-15063**

Ollama MCP Server execAsync Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ollama MCP Server. Authentication is not required to exploit this vulnerability

9.8 **CVE-2026-0756**

github-kanban-mcp-server execAsync Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of github-kanban-mcp-server. Authentication is not required to exploit this

9.8 **CVE-2026-0759**

Katana Network Development Starter Kit executeCommand Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Katana Network Development Starter Kit. Authenticatio

9.8 **CVE-2026-0760** Deepwisdom metagpt

Foundation Agents MetaGPT deserialize_message Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foundation Agents MetaGPT. Authentication is

9.8 **CVE-2026-0773**

Upsonic Cloudpickle Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Upsonic. Authentication is not required to exploit this vulnerability.

9.8 **CVE-2026-0787** Algosolutions 8180 ip audio alerter firmware

ALGO 8180 IP Audio Alerter SAC Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of ALGO 8180 IP Audio Alerter devices. Authentication is not required to exploi

9.8 **CVE-2026-0763** Binary-Husky gpt academic

GPT Academic run_in_subprocess_wrapper_func Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GPT Academic. Authentication is not required to

9.8 **CVE-2026-0764** Binary-Husky gpt academic

GPT Academic upload Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GPT Academic. Authentication is not required to exploit this vulnerabil

9.8 **CVE-2021-47891**

Unified Remote 3.9.0.2463 contains a remote code execution vulnerability that allows attackers to send crafted network packets to execute arbitrary commands. Attackers can exploit the service by connecting to port 9512 and sending specially crafted packets to

9.8 **CVE-2025-70457** Remyandrade modern image gallery app

A Remote Code Execution (RCE) vulnerability exists in Sourcecodester Modern Image Gallery App v1.0 within the gallery/upload.php component. The application fails to properly validate uploaded file contents. Additionally, the application preserves the user-supp

15 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.