Daily brief, Wednesday, January 14, 2026

Jan 13, 7:00 PM to Jan 14, 7:00 PM ET

Generated Nov 8, 2026, 11:23 PM ET

0	0	0	18	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

18 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

18

9.8 **CVE-2025-37184** Arubanetworks edgeconnect sd-wan orchestrator

A vulnerability exists in an Orchestrator service that could allow an unauthenticated remote attacker to bypass multi-factor authentication requirements. Successful exploitation could allow an attacker to create an admin user account without the necessary mult

9.1 **CVE-2025-71116** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: libceph: make decode_pool() more resilient against corrupted osdmaps If the osdmap is (maliciously) corrupted such that the encoded length of ceph_pg_pool envelope is less than what is expecte

9.8 **CVE-2026-23550** DETECTION

Incorrect Privilege Assignment vulnerability in Modular DS Modular DS modular-connector allows Privilege Escalation.This issue affects Modular DS: from n/a through <= 2.5.1.

9.8 **CVE-2025-14502**

The News and Blog Designer Bundle plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1 via the template parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files

9.1 **CVE-2026-22855** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a heap out-of-bounds read occurs in the smartcard SetAttrib path when cbAttrLen does not match the actual NDR buffer length. This vulnerability is fixed in 3.20.1.

9.1 **CVE-2026-22859** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, the URBDRC client does not perform bounds checking on server?supplied MSUSB_INTERFACE_DESCRIPTOR values and uses them as indices in libusb_udev_complete_msconfig_setup, causing a

9.8 **CVE-2026-22708** Anysphere cursor

Cursor is a code editor built for programming with AI. Prior to 2.3, hen the Cursor Agent is running in Auto-Run Mode with Allowlist mode enabled, certain shell built-ins can still be executed without appearing in the allowlist and without requiring user appro

9.8 **CVE-2026-22853** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, RDPEAR’s NDR array reader does not perform bounds checking on the on?wire element count and can write past the heap buffer allocated from hints, causing a heap buffer overflow in

10.0 **CVE-2026-22686** Agentfront enclave

Enclave is a secure JavaScript sandbox designed for safe AI agent code execution. Prior to 2.7.0, there is a critical sandbox escape vulnerability in enclave-vm that allows untrusted, sandboxed JavaScript code to execute arbitrary code in the host Node.js runt

9.8 **CVE-2026-22238** Blusparkglobal bluvoyix

The vulnerability exists in BLUVOYIX due to improper authentication in the BLUVOYIX admin APIs. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable admin API to create a new user with

9.1 **CVE-2026-22858** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, global-buffer-overflow was observed in FreeRDP's Base64 decoding path. The root cause appears to be implementation-defined char signedness: on Arm/AArch64 builds, plain char is t

9.8 **CVE-2025-14301**

The Integration Opvius AI for WooCommerce plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.3.0. This is due to the `process_table_bulk_actions()` function processing user-supplied file paths without authentication ch

9.8 **CVE-2026-22236** Blusparkglobal bluvoyix

The vulnerability exists in BLUVOYIX due to improper authentication in the BLUVOYIX backend APIs. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable APIs. Successful exploitation of

9.8 **CVE-2026-22854** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a heap-buffer-overflow occurs in drive read when a server-controlled read length is used to read file data into an IRP output stream buffer without a hard upper bound, allowing a

9.8 **CVE-2026-22857** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a heap use-after-free occurs in irp_thread_func because the IRP is freed by irp->Complete() and then accessed again on the error path. This vulnerability is fixed in 3.20.1.

9.8 **CVE-2025-70968** Freeimage Project freeimage

FreeImage 3.18.0 contains a Use After Free in PluginTARGA.cpp;loadRLE().

9.8 **CVE-2026-22237** Blusparkglobal bluvoyix

The vulnerability exists in BLUVOYIX due to the exposure of sensitive internal API documentation. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the APIs exposed by the documentation. Successfu

9.8 **CVE-2026-22852** Freerdp freerdp

FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.20.1, a malicious RDP server can trigger a heap-buffer-overflow write in the FreeRDP client when processing Audio Input (AUDIN) format lists. audin_process_formats reuses callback->for

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.