Daily brief, Tuesday, November 25, 2025

Nov 24, 7:00 PM to Nov 25, 7:00 PM ET

Generated Nov 9, 2026, 7:27 AM ET

0	0	0	20	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

20 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

20

9.8 **CVE-2025-6389** DETECTION

The Sneeit Framework plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 8.3 via the sneeit_articles_pagination_callback() function. This is due to the function accepting user input and then passing that through ca

9.2 **CVE-2025-59366**

An authentication-bypass vulnerability exists in AiCloud. This vulnerability can be triggered by an unintended side effect of the Samba functionality, potentially leading to allow execution of specific functions without proper authorization. Refer to the Secur

9.8 **CVE-2025-13595**

The CIBELES AI plugin for WordPress is vulnerable to arbitrary file uploads due to missing capability check in the 'actualizador_git.php' file in all versions up to, and including, 1.10.8. This makes it possible for unauthenticated attackers to download arbitr

9.8 **CVE-2025-13597**

The AI Feeds plugin for WordPress is vulnerable to arbitrary file uploads due to missing capability check in the 'actualizador_git.php' file in all versions up to, and including, 1.0.11. This makes it possible for unauthenticated attackers to download arbitrar

9.8 **CVE-2025-62691**

Security Point (Windows) of MaLion and MaLionCloud contains a stack-based buffer overflow vulnerability in processing HTTP headers. Receiving a specially crafted request from a remote unauthenticated attacker could lead to arbitrary code execution with SYSTEM

9.8 **CVE-2025-64693**

Security Point (Windows) of MaLion and MaLionCloud contains a heap-based buffer overflow vulnerability in processing Content-Length. Receiving a specially crafted request from a remote unauthenticated attacker could lead to arbitrary code execution with SYSTEM

9.8 **CVE-2025-61168** Sigb pmb

An issue in the cms_rest.php component of SIGB PMB v8.0.1.14 allows attackers to execute arbitrary code via unserializing an arbitrary file.

9.8 **CVE-2025-51742** Jishenghua jsherp

An issue was discovered in jishenghua JSH_ERP 2.3.1. The /material/getMaterialEnableSerialNumberList endpoint passes the search query parameter directly to parseObject(), introducing a Fastjson deserialization vulnerability that can lead to RCE via JDBC payloa

9.8 **CVE-2025-51743** Jishenghua jsherp

An issue was discovered in jishenghua JSH_ERP 2.3.1. The /materialCategory/addMaterialCategory endpoint is vulnerable to fastjson deserialization attacks.

9.8 **CVE-2025-51744** Jishenghua jsherp

An issue was discovered in jishenghua JSH_ERP 2.3.1. The /user/addUser endpoint is vulnerable to fastjson deserialization attacks.

9.8 **CVE-2025-51745** Jishenghua jsherp

An issue was discovered in jishenghua JSH_ERP 2.3.1. The /role/addcan endpoint is vulnerable to fastjson deserialization attacks.

9.8 **CVE-2025-51746** Jishenghua jsherp

An issue was discovered in jishenghua JSH_ERP 2.3.1. The /serialNumber/addSerialNumber endpoint is vulnerable to fastjson deserialization attacks.

9.8 **CVE-2025-65085** Ashlar argon

A Heap-based Buffer Overflow vulnerability is present in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions 12.6.1204.216 and prior that could allow an attacker to disclose information or execute arbitrary code.

9.8 **CVE-2025-64063** Primakon project contract management

Primakon Pi Portal 1.0.18 API endpoints fail to enforce sufficient authorization checks when processing requests. Specifically, a standard user can exploit this flaw by sending direct HTTP requests to administrative endpoints, bypassing the UI restrictions. Th

9.8 **CVE-2025-13559**

The EduKart Pro plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.3. This is due to the 'edukart_pro_register_user_front_end' function not restricting what user roles a user can register with. This makes it po

9.8 **CVE-2025-65084** Ashlar argon

An Out-of-Bounds Write vulnerability is present in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions 12.6.1204.216 and prior that could allow an attacker to disclose information or execute arbitrary code.

9.6 **CVE-2025-60739** Ilevia eve x1 server firmware

Cross Site Request Forgery (CSRF) vulnerability in Ilevia EVE X1 Server Firmware Version v4.7.18.0.eden and before, Logic Version v6.00 - 2025_07_21 allows a remote attacker to execute arbitrary code via the /bh_web_backend component

9.3 **CVE-2025-66016**

CGGMP24 is a state-of-art ECDSA TSS protocol that supports 1-round signing (requires 3 preprocessing rounds), identifiable abort, and a key refresh protocol. Prior to version 0.6.3, there is a missing check in the ZK proof that enables an attack in which singl

9.3 **CVE-2025-33187** Nvidia dgx os

NVIDIA DGX Spark GB10 contains a vulnerability in SROOT, where an attacker could use privileged access to gain access to SoC protected areas. A successful exploit of this vulnerability might lead to code execution, information disclosure, data tampering, denia

9.0 **CVE-2025-63729** Syrotech sy-gpon-1110-wdont firmware

An issue was discovered in Syrotech SY-GPON-1110-WDONT SYRO_3.7L_3.1.02-240517 allowing attackers to exctract the SSL Private Key, CA Certificate, SSL Certificate, and Client Certificates in .pem format in firmware in etc folder.

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.