Daily brief, Monday, December 1, 2025

Nov 30, 7:00 PM to Dec 1, 7:00 PM ET

Generated Nov 9, 2026, 6:32 AM ET

0	0	0	13	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

13 new critical CVEs, 1 new breaches.

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

13

9.1 **CVE-2025-12106** Openvpn openvpn

Insufficient argument validation in OpenVPN 2.7_alpha1 through 2.7_rc1 allows an attacker to trigger a heap buffer over-read when parsing IP addresses

9.8 **CVE-2025-66401** Kapilduraphe mcp watch

MCP Watch is a comprehensive security scanner for Model Context Protocol (MCP) servers. In 0.1.2 and earlier, the MCPScanner class contains a critical Command Injection vulnerability in the cloneRepo method. The application passes the user-supplied githubUrl a

9.8 **CVE-2025-51683** Mjobtime mjobtime DETECTION

A blind SQL Injection (SQLi) vulnerability in mJobtime v15.7.2 allows unauthenticated attackers to execute arbitrary SQL statements via a crafted POST request to the /Default.aspx/update_profile_Server endpoint .

9.8 **CVE-2025-51682** Mjobtime mjobtime

mJobtime 15.7.2 handles authorization on the client side, which allows an attacker to modify the client-side code and gain access to administrative features. Additionally, they can craft requests based on the client-side code to call these administrative funct

9.6 **CVE-2025-66301** Getgrav grav

Grav is a file-based Web platform. Prior to 1.8.0-beta.27, due to improper authorization checks when modifying critical fields on a POST request to /admin/pages/{page_name}, an editor with only permissions to change basic content on the form is now able to cha

10.0 **CVE-2025-63531** Shridharshukl blood bank management system

A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the receiverLogin.php component. The application fails to properly sanitize user-supplied input in SQL queries, allowing an attacker to inject arbitrary SQL code. By manipulati

9.1 **CVE-2025-66410** Gin-Vue-Admin Project gin-vue-admin

Gin-vue-admin is a backstage management system based on vue and gin. In 2.8.6 and earlier, attackers can delete any file on the server at will, causing damage or unavailability of server resources. Attackers can control the 'FileMd5' parameter to delete any fi

9.6 **CVE-2025-63525** Shridharshukl blood bank management system

An issue was discovered in Blood Bank Management System 1.0 allowing authenticated attackers to perform actions with escalated privileges via crafted request to delete.php.

9.0 **CVE-2025-3500** Avast antivirus

Integer Overflow or Wraparound vulnerability in Avast Antivirus (25.1.981.6) on Windows allows Privilege Escalation.This issue affects Antivirus: from 25.1.981.6 before 25.3.

9.6 **CVE-2025-63532** Shridharshukl blood bank management system

A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the cancel.php component. The application fails to properly sanitize user-supplied input in SQL queries, allowing an attacker to inject arbitrary SQL code. By manipulating the

9.6 **CVE-2025-63535** Shridharshukl blood bank management system

A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the abs.php component. The application fails to properly sanitize usersupplied input in SQL queries, allowing an attacker to inject arbitrary SQL code. By manipulating the sear

9.8 **CVE-2025-66405** Portkey gateway

Portkey.ai Gateway is a blazing fast AI Gateway with integrated guardrails. Prior to 1.14.0, the gateway determined the destination baseURL by prioritizing the value in the x-portkey-custom-host request header. The proxy route then appends the client-specified

9.1 **CVE-2025-65836** Publiccms publiccms

PublicCMS V5.202506.b is vulnerable to SSRF. in the chat interface of SimpleAiAdminController.

Ransomware

No leak-site posts collected.

New data breaches 1

Zilvia.net zilvia.net 287,863 accounts

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.