Daily brief, Tuesday, January 13, 2026

Jan 12, 7:00 PM to Jan 13, 7:00 PM ET

Generated Nov 8, 2026, 11:35 PM ET

0	1	0	50	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 50 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

5.5 **CVE-2026-20805** Microsoft Windows CISA KEV

A locally authorized attacker can disclose information from Microsoft Windows via the Desktop Window Manager component.

New public exploit code

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

New critical CVEs

50

9.8 **CVE-2023-54335** Extplorer eXtplorer EXPLOIT CODE DETECTION

Affected: eXtplorer 2.1.14 (PHP-based web file manager) login/authentication logic. Attacker gains: unauthenticated login without a password, then can upload PHP files and achieve remote code execution, with full control of the hosting web server's files and d

9.8 **CVE-2025-64155** Fortinet fortisiem DETECTION

An improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSIEM 7.4.0, FortiSIEM 7.3.0 through 7.3.4, FortiSIEM 7.1.0 through 7.1.8, FortiSIEM 7.0.0 through 7.0.4, FortiSIEM 6.7.0 through 6.7.10

9.8 **CVE-2025-69992** Phpgurukul news portal

phpgurukul News Portal Project V4.1 has File Upload Vulnerability via upload.php, which enables the upload of files of any format to the server without identity authentication.

9.8 **CVE-2026-0879** Mozilla firefox

Sandbox escape due to incorrect boundary conditions in the Graphics component. This vulnerability was fixed in Firefox 147, Firefox ESR 115.32, Firefox ESR 140.7, Thunderbird 147, and Thunderbird 140.7.

9.1 **CVE-2026-0498** Sap s\/4 hana

SAP S/4HANA (Private Cloud and On-Premise) allows an attacker with admin privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code/OS commands into the system, bypassing essential autho

9.8 **CVE-2025-69991** Phpgurukul news portal

phpgurukul News Portal Project V4.1 is vulnerable to SQL Injection in check_availablity.php.

9.8 **CVE-2026-0884** Mozilla firefox

Use-after-free in the JavaScript Engine component. This vulnerability was fixed in Firefox 147, Firefox ESR 140.7, Thunderbird 147, and Thunderbird 140.7.

9.1 **CVE-2025-69990** Phpgurukul news portal

phpgurukul News Portal Project V4.1 has an Arbitrary File Deletion Vulnerability in remove_file.php. The parameter file can cause any file to be deleted.

9.8 **CVE-2026-0892** Mozilla firefox

Memory safety bugs present in Firefox 146 and Thunderbird 146. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox

9.8 **CVE-2025-68817** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_tree_connect_put under concurrency Under high concurrency, A tree-connection object (tcon) is freed on a disconnect path while another path still holds a ref

9.6 **CVE-2026-0500** Sap introscope enterprise manager

Due to the usage of vulnerable third party component in SAP Wily Introscope Enterprise Manager (WorkStation), an unauthenticated attacker could create a malicious JNLP (Java Network Launch Protocol) file accessible by a public facing URL. When a victim clicks

9.8 **CVE-2025-71068** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: svcrdma: bound check rq_pages index in inline path svc_rdma_copy_inline_range indexed rqstp->rq_pages[rc_curpage] without verifying rc_curpage stays within the allocated page array. Add guards

10.0 **CVE-2026-0881** Mozilla firefox

Sandbox escape in the Messaging System component. This vulnerability was fixed in Firefox 147 and Thunderbird 147.

9.1 **CVE-2025-71093** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: e1000: fix OOB in e1000_tbi_should_accept() In e1000_tbi_should_accept() we read the last byte of the frame via 'data[length - 1]' to evaluate the TBI workaround. If the descriptor- reported l

9.1 **CVE-2025-71095** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: stmmac: fix the crash issue for zero copy XDP_TX action There is a crash issue when running zero copy XDP_TX action, the crash log is shown below. [216.122464] Unable to handle kernel pa

9.3 **CVE-2026-22755**

Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Vivotek Affected device model numbers are FD8365, FD8365v2, FD9165, FD9171, FD9187, FD9189, FD9365, FD9371, FD9381, FD9387, FD9389, FD9391,FE9180,FE9181, FE919

9.8 **CVE-2020-36911** Cobbr covenant

Covenant 0.1.3 - 0.5 contains a remote code execution vulnerability that allows attackers to craft malicious JWT tokens with administrative privileges. Attackers can generate forged tokens with admin roles and upload custom DLL payloads to execute arbitrary co

9.8 **CVE-2023-54339** Webgrind Project webgrind

Webgrind 1.1 contains a remote command execution vulnerability that allows unauthenticated attackers to inject OS commands via the dataFile parameter in index.php. Attackers can execute arbitrary system commands by manipulating the dataFile parameter, such as

9.1 **CVE-2025-11250** Zohocorp manageengine adselfservice plus

Zohocorp ManageEngine ADSelfService Plus versions before 6519 are vulnerable to Authentication Bypass due to improper filter configurations.

9.8 **CVE-2022-50919** Tdarr tdarr

Tdarr 2.00.15 contains an unauthenticated remote code execution vulnerability in its Help terminal that allows attackers to inject and chain arbitrary commands. Attackers can exploit the lack of input filtering by chaining commands like `--help; curl .py | pyt

30 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.