Daily brief, Wednesday, December 24, 2025

Dec 23, 7:00 PM to Dec 24, 7:00 PM ET

Generated Nov 9, 2026, 2:54 AM ET

0	0	0	24	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

24 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

24

9.8 **CVE-2025-13773** DETECTION

The Print Invoice & Delivery Notes for WooCommerce plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 5.8.0 via the 'WooCommerce_Delivery_Notes::update' function. This is due to missing capability check in the 'Wo

9.1 **CVE-2025-68916** Riello-Ups netman 208

Riello UPS NetMan 208 Application before 1.12 allows cgi-bin/certsupload.cgi /../ directory traversal for file upload with resultant code execution.

9.8 **CVE-2025-8769**

Telenium Online Web Application is vulnerable due to a Perl script that is called to load the login page. Due to improper input validation, an attacker can inject arbitrary Perl code through a crafted HTTP request, leading to remote code execution on the serve

9.8 **CVE-2022-50717**

In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: add bounds check on Transfer Tag ttag is used as an index to get cmd in nvmet_tcp_handle_h2c_data_pdu(), add a bounds check to avoid out-of-bounds access.

9.8 **CVE-2019-25241** Iwt facesentry access control system firmware

FaceSentry Access Control System 6.4.8 contains a critical authentication vulnerability with hard-coded SSH credentials for the wwwuser account. Attackers can leverage the insecure sudoers configuration to escalate privileges and gain root access by executing

9.8 **CVE-2018-25135**

Anviz AIM CrossChex Standard 4.3.6.0 contains a CSV injection vulnerability that allows attackers to execute commands by inserting malicious formulas in user import fields. Attackers can craft payloads in fields like 'Name', 'Gender', or 'Position' to trigger

9.8 **CVE-2018-25134**

Synaccess netBooter NP-02x/NP-08x 6.8 contains an authentication bypass vulnerability in the webNewAcct.cgi script that allows unauthenticated attackers to create admin user accounts. Attackers can exploit the missing control check by sending crafted POST requ

9.8 **CVE-2025-68359**

In the Linux kernel, the following vulnerability has been resolved: btrfs: fix double free of qgroup record after failure to add delayed ref head In the previous code it was possible to incur into a double kfree() scenario when calling add_delayed_ref_head().

9.8 **CVE-2018-25138** Flir flir ax8 firmware

FLIR AX8 Thermal Camera 1.32.16 contains hard-coded SSH and web panel credentials that cannot be changed through normal camera operations. Attackers can exploit these persistent credentials to gain unauthorized shell access and login to multiple camera interfa

9.8 **CVE-2023-54090**

In the Linux kernel, the following vulnerability has been resolved: ixgbe: Fix panic during XDP_TX with > 64 CPUs Commit 4fe815850bdc ("ixgbe: let the xdpdrv work with more than 64 cpus") adds support to allow XDP programs to run on systems with more than 64 C

9.8 **CVE-2023-54094**

In the Linux kernel, the following vulnerability has been resolved: net: prevent skb corruption on frag list segmentation Ian reported several skb corruptions triggered by rx-gro-list, collecting different oops alike: [62.624003] BUG: kernel NULL pointer dere

9.8 **CVE-2023-53867**

In the Linux kernel, the following vulnerability has been resolved: ceph: fix potential use-after-free bug when trimming caps When trimming the caps and just after the 'session->s_cap_lock' is released in ceph_iterate_session_caps() the cap maybe removed by an

9.8 **CVE-2025-68745**

In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Clear cmds after chip reset Commit aefed3e5548f ("scsi: qla2xxx: target: Fix offline port handling and host reset handling") caused two problems: 1. Commands sent to FW, after c

9.8 **CVE-2019-25235**

Smartwares HOME easy 1.0.9 contains an authentication bypass vulnerability that allows unauthenticated attackers to access administrative web pages by disabling JavaScript. Attackers can navigate to multiple administrative endpoints and to bypass client-side v

9.8 **CVE-2019-25240**

Rifatron 5brid DVR contains an unauthenticated vulnerability in the animate.cgi script that allows unauthorized access to live video streams. Attackers can exploit the Mobile Web Viewer module by specifying channel numbers to retrieve sequential video snapshot

9.8 **CVE-2023-54076**

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix missed ses refcounting Use new cifs_smb_ses_inc_refcount() helper to get an active reference of @ses and @ses->dfs_root_ses (if set). This will prevent @ses->dfs_root_ses of b

9.8 **CVE-2019-25236**

iSeeQ Hybrid DVR WH-H4 1.03R contains an unauthenticated vulnerability in the get_jpeg script that allows unauthorized access to live video streams. Attackers can retrieve video snapshots from specific camera channels by sending requests to the /cgi-bin/get_jp

9.8 **CVE-2018-25142**

NovaRad NovaPACS Diagnostics Viewer 8.5.19.75 contains an unauthenticated XML External Entity (XXE) injection vulnerability in XML preference import settings. Attackers can craft malicious XML files with DTD parameter entities to retrieve arbitrary system file

9.8 **CVE-2025-68741**

In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix improper freeing of purex item In qla2xxx_process_purls_iocb(), an item is allocated via qla27xx_copy_multiple_pkt(), which internally calls qla24xx_alloc_purex_item(). The

9.8 **CVE-2019-25249**

devolo dLAN 500 AV Wireless+ 3.1.0-1 contains an authentication bypass vulnerability that allows attackers to enable hidden services through the htmlmgr CGI script. Attackers can enable telnet and remote shell services, reboot the device, and gain root access

4 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

?????????? ?????????? ???????? (Gemotest)	gemotest.ru	6,341,495 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.