Daily brief, Tuesday, December 30, 2025

Dec 29, 7:00 PM to Dec 30, 7:00 PM ET

Generated Nov 9, 2026, 1:56 AM ET

0	0	0	29	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

29 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

29

9.8 **CVE-2025-68926** Rustfs rustfs

RustFS is a distributed object storage system built in Rust. In versions prior to 1.0.0-alpha.78, RustFS implements gRPC authentication using a hardcoded static token `"rustfs rpc"` that is publicly exposed in the source code repository, hardcoded on both clie

9.8 **CVE-2025-15255** Tenda w6-s firmware

A vulnerability was determined in Tenda W6-S 1.0.0.4(510). This impacts an unknown function of the file /bin/httpd of the component R7websSsecurityHandler. Executing a manipulation of the argument Cookie can lead to stack-based buffer overflow. The attack may

9.8 **CVE-2022-50794** Sound4 impact firmware

SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain an unauthenticated command injection vulnerability in the username parameter. Attackers can exploit index.php and login.php scripts by injecting arbitrary shell commands through the HTTP POST 'userna

9.8 **CVE-2022-50796** Sound4 impact firmware

SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x contains an unauthenticated remote code execution vulnerability in the firmware upload functionality with path traversal flaw. Attackers can exploit the upload.cgi script to write malicious files to the system with www-data

9.8 **CVE-2022-50691** Minidvblinux minidvblinux

MiniDVBLinux 5.4 contains a remote command execution vulnerability that allows unauthenticated attackers to execute arbitrary commands as root through the 'command' GET parameter. Attackers can exploit the /tpl/commands.sh endpoint by sending malicious command

9.8 **CVE-2025-66848** Jdcloud ax1800 firmware

JD Cloud NAS routers AX1800 (4.3.1.r4308 and earlier), AX3000 (4.3.1.r4318 and earlier), AX6600 (4.5.1.r4533 and earlier), BE6500 (4.4.1.r4308 and earlier), ER1 (4.5.1.r4518 and earlier), and ER2 (4.5.1.r4518 and earlier) contain an unauthorized remote command

9.8 **CVE-2022-50694** Sound4 impact firmware

SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x contains an SQL injection vulnerability in the 'username' POST parameter of index.php that allows attackers to manipulate database queries. Attackers can inject arbitrary SQL code through the username parameter to bypass aut

10.0 **CVE-2024-58338** Ateme flamingo xl firmware

Anevia Flamingo XL 3.2.9 contains a restricted shell vulnerability that allows remote attackers to escape the sandboxed environment through the traceroute command. Attackers can exploit the traceroute command to inject shell commands and gain full root access

9.8 **CVE-2023-54327** Tinycontrol lan controller firmware

Tinycontrol LAN Controller 1.58a contains an authentication bypass vulnerability that allows unauthenticated attackers to change admin passwords through a crafted API request. Attackers can exploit the /stm.cgi endpoint with a specially crafted authentication

9.8 **CVE-2023-53983** Ateme flamingo xl firmware

Anevia Flamingo XL/XS 3.6.20 contains a critical vulnerability with weak default administrative credentials that can be easily guessed. Attackers can leverage these hard-coded credentials to gain full remote system control without complex authentication mechan

9.8 **CVE-2023-54257**

In the Linux kernel, the following vulnerability has been resolved: net: macb: fix a memory corruption in extended buffer descriptor mode For quite some time we were chasing a bug which looked like a sudden permanent failure of networking and mmc on some of ou

9.8 **CVE-2022-50696** Sound4 first firmware

SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain hardcoded credentials embedded in server binaries that cannot be modified through normal device operations. Attackers can leverage these static credentials to gain unauthorized access to the device a

9.8 **CVE-2025-15111** Kseniasecurity lares firmware

Ksenia Security lares (legacy model) version 1.6 contains a default credentials vulnerability that allows unauthorized attackers to gain administrative access. Attackers can exploit the weak default administrative credentials to obtain full control of the home

9.8 **CVE-2023-54184**

In the Linux kernel, the following vulnerability has been resolved: scsi: target: iscsit: Free cmds before session free Commands from recovery entries are freed after session has been closed. That leads to use-after-free at command free or NPE with such call t

9.8 **CVE-2023-54237**

In the Linux kernel, the following vulnerability has been resolved: net/smc: fix potential panic dues to unprotected smc_llc_srv_add_link() There is a certain chance to trigger the following panic: PID: 5900 TASK: ffff88c1c8af4100 CPU: 1 COMMAND: "kworker/1:48

9.8 **CVE-2023-54258**

In the Linux kernel, the following vulnerability has been resolved: cifs: fix potential oops in cifs_oplock_break With deferred close we can have closes that race with lease breaks, and so with the current checks for whether to send the lease response, oplock_

9.8 **CVE-2025-15114** Kseniasecurity lares firmware

Ksenia Security lares (legacy model) Home Automation version 1.6 contains a critical security flaw that exposes the alarm system PIN in the 'basisInfo' XML file after authentication. Attackers can retrieve the PIN from the server response to bypass security me

9.8 **CVE-2023-54269**

In the Linux kernel, the following vulnerability has been resolved: SUNRPC: double free xprt_ctxt while still in use When an RPC request is deferred, the rq_xprt_ctxt pointer is moved out of the svc_rqst into the svc_deferred_req. When the deferred request is

9.8 **CVE-2023-54292**

In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Fix data race on CQP request done KCSAN detects a data race on cqp_request->request_done memory location which is accessed locklessly in irdma_handle_cqp_op while being updated in

9.1 **CVE-2023-54203**

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix slab-out-of-bounds in init_smb2_rsp_hdr When smb1 mount fails, KASAN detect slab-out-of-bounds in init_smb2_rsp_hdr like the following one. For smb1 negotiate(56bytes) , init_smb2_r

9 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.