Daily brief, Monday, December 22, 2025

Dec 21, 7:00 PM to Dec 22, 7:00 PM ET

Generated Nov 9, 2026, 3:14 AM ET

0	1	0	22	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 22 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.8 **CVE-2023-52163** Digiever DS-2105 Pro CISA KEV DETECTION

Missing authorization in the Digiever DS-2105 Pro lets an attacker inject OS commands through the time_tzsetup.cgi endpoint.

New public exploit code

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

New critical CVEs

22

9.8 **CVE-2023-53963** Sound4 impact firmware

SOUND4 IMPACT/FIRST/PULSE/Eco v2.x contains an unauthenticated OS command injection vulnerability that allows remote attackers to execute arbitrary shell commands through the 'password' parameter. Attackers can exploit the login.php and index.php scripts by in

9.8 **CVE-2025-15007** Tenda wh450 firmware

A security vulnerability has been detected in Tenda WH450 1.0.0.18. Affected by this issue is some unknown functionality of the file /goform/L7Im of the component HTTP Request Handler. Such manipulation of the argument page leads to stack-based buffer overflow

9.8 **CVE-2025-15010** Tenda wh450 firmware

A vulnerability has been found in Tenda WH450 1.0.0.18. This issue affects some unknown processing of the file /goform/SafeUrlFilter. The manipulation of the argument page leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The

9.8 **CVE-2023-53964** Sound4 impact firmware

SOUND4 IMPACT/FIRST/PULSE/Eco v2.x contains an unauthenticated vulnerability in the /usr/cgi-bin/restorefactory.cgi endpoint that allows remote attackers to reset device configuration. Attackers can send a POST request to the endpoint with specific data to tri

9.8 **CVE-2025-15006** Tenda wh450 firmware

A weakness has been identified in Tenda WH450 1.0.0.18. Affected by this vulnerability is an unknown functionality of the file /goform/CheckTools of the component HTTP Request Handler. This manipulation of the argument ipaddress causes stack-based buffer overf

9.8 **CVE-2023-53980** Projectsend projectsend

ProjectSend r1605 contains a remote code execution vulnerability that allows attackers to upload malicious files by manipulating file extensions. Attackers can upload shell scripts with disguised extensions through the upload.process.php endpoint to execute ar

9.8 **CVE-2023-53955** Sound4 stream extension

SOUND4 IMPACT/FIRST/PULSE/Eco v2.x contains an insecure direct object reference vulnerability that allows attackers to bypass authorization and access hidden system resources. Attackers can exploit the vulnerability by manipulating user-supplied input to execu

9.8 **CVE-2025-65856** Xiongmaitech xm530v200 x6-weq 8m firmware

Authentication bypass vulnerability in Xiongmai XM530 IP cameras on Firmware V5.00.R02.000807D8.10010.346624.S.ONVIF 21.06 allows unauthenticated remote attackers to access sensitive device information and live video streams. The ONVIF implementation fails to

9.8 **CVE-2023-53960** Sound4 first firmware

SOUND4 IMPACT/FIRST/PULSE/Eco version 2.x contains an SQL injection vulnerability in the 'index.php' authentication mechanism that allows attackers to manipulate login credentials. Attackers can inject malicious SQL code through the 'password' POST parameter t

9.8 **CVE-2023-53966** Sound4 linkandshare transmitter

SOUND4 LinkAndShare Transmitter 1.1.2 contains a format string vulnerability that allows attackers to trigger memory stack overflows through maliciously crafted environment variables. Attackers can manipulate the username environment variable with format strin

9.8 **CVE-2023-53968** Dbbroadcast sft dab 600\/c firmware

Screen SFT DAB 600/C Firmware 1.9.3 contains a session management vulnerability that allows attackers to bypass authentication controls by exploiting IP address session binding. Attackers can reuse the same IP address and issue unauthorized requests to the use

9.6 **CVE-2024-27708** Airc mynet

Iframe injection vulnerability in airc.pt/solucoes-servicos.solucoes MyNET v.26.06 and before allows a remote attacker to execute arbitrary code via the src parameter.

10.0 **CVE-2025-67288** Umbraco umbraco cms

An arbitrary file upload vulnerability in Umbraco CMS v16.3.3 allows attackers to execute arbitrary code by uploading a crafted PDF file. NOTE: this is disputed by the Supplier because the responsibility for file validation (as shown in the documentation) belo

9.8 **CVE-2025-15016** Ragic enterprise cloud database

Enterprise Cloud Database developed by Ragic has a Hard-coded Cryptographic Key vulnerability, allowing unauthenticated remote attackers to exploit the fixed key to generate verification information and log into the system as any user.

9.8 **CVE-2025-67418** Oxygenz clipbucket

ClipBucket 5.5.2 is affected by an improper access control issue where the product is shipped or deployed with hardcoded default administrative credentials. An unauthenticated remote attacker can log in to the administrative panel using these default credentia

9.6 **CVE-2025-67289** Frappe erpnext

An arbitrary file upload vulnerability in the Attachments module of Frappe Framework v15.89.0 allows attackers to execute arbitrary code via uploading a crafted XML file.

9.8 **CVE-2025-11541** Sharp np-p502h firmware

+1 more CVEs in the same release

Stack-based Buffer Overflow vulnerability in Sharp Display Solutions projectors allows a attacker may execute arbitrary commands and programs.

9.8 **CVE-2025-12049** Sharp mp-01 firmware

Missing Authentication for Critical Function vulnerability in Sharp Display Solutions Media Player MP-01 All Verisons allows a attacker may access to the web interface of the affected product without authentication and change settings or perform other operatio

9.5 **CVE-2025-11544**

Improper Validation of Integrity Check Value vulnerability in Sharp Display Solutions projectors allows a attacker may create and run unauthorized firmware.

9.5 **CVE-2025-11545**

Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Sharp Display Solutions projectors allows a attacker may improperly access the HTTP server and execute arbitrary actions.

1 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.