Daily brief, Monday, January 12, 2026

Jan 11, 7:00 PM to Jan 12, 7:00 PM ET

Generated Nov 8, 2026, 11:52 PM ET

0	1	0	21	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 21 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.7 **CVE-2025-8110** Gogs Gogs CISA KEV DETECTION

Gogs path traversal in the PutContents API, via improper symbolic link handling, lets an attacker achieve code execution.

New public exploit code

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

New critical CVEs

21

9.8 **CVE-2025-12420** Servicenow now assist ai agents DETECTION

A vulnerability has been identified in the ServiceNow AI Platform that could enable an unauthenticated user to impersonate another user and perform the operations that the impersonated user is entitled to perform. ServiceNow has addressed this vulnerability by

10.0 **CVE-2025-52694** Advantech iot edge linux docker DETECTION

Successful exploitation of the SQL injection vulnerability could allow an unauthenticated remote attacker to execute arbitrary SQL commands on the vulnerable service when it is exposed to the Internet, potentially affecting data confidentiality, integrity, and

9.1 **CVE-2026-22252** Librechat librechat

LibreChat is a ChatGPT clone with additional features. Prior to v0.8.2-rc2, LibreChat's MCP stdio transport accepts arbitrary commands without validation, allowing any authenticated user to execute shell commands as root inside the container through a single A

9.8 **CVE-2026-22781** Ritlabs tinyweb

TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. TinyWeb HTTP Server before version 1.98 is vulnerable to OS command injection via CGI ISINDEX-style query parameters. The query parameters are passed as command-line arguments to the CGI execut

9.8 **CVE-2025-29329** Sagemcom f\@st 3686 firmware

Buffer Overflow in the ippprint (Internet Printing Protocol) service in Sagemcom F@st 3686 MAGYAR_4.121.0 allows remote attacker to execute arbitrary code by sending a crafted HTTP request.

9.8 **CVE-2025-66802** Covid-19 Contact Tracing System Project covid-19 contact tracing system

Sourcecodester Covid-19 Contact Tracing System 1.0 is vulnerable to RCE (Remote Code Execution). The application receives a reverse shell (php) into imagem of the user enabling RCE.

9.8 **CVE-2025-69269** Broadcom dx netops spectrum

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows OS Command Injection.This issue affects DX NetOps Spectrum: 23.3.6 and earlier.

9.8 **CVE-2026-22785** Orval orval

orval generates type-safe JS clients (TypeScript) from any valid OpenAPI v3 or Swagger v2 specification. Prior to 7.18.0, the MCP server generation logic relies on string manipulation that incorporates the summary field from the OpenAPI specification without p

9.4 **CVE-2025-67146** Abhishekmali21 gym management system

Multiple SQL Injection vulnerabilities exist in AbhishekMali21 GYM-MANAGEMENT-SYSTEM 1.0 via the 'name' parameter in (1) member_search.php, (2) trainer_search.php, and (3) gym_search.php, and via the 'id' parameter in (4) payment_search.php. An unauthenticated

9.8 **CVE-2025-46070** Automai botmanager

An issue in Automai BotManager v.25.2.0 allows a remote attacker to execute arbitrary code via the BotManager.exe component

9.8 **CVE-2026-22214** Riot-Os riot

RIOT OS versions up to and including 2026.01-devel-317 contain a stack-based buffer overflow vulnerability in the ethos utility due to missing bounds checking when processing incoming serial frame data. The vulnerability occurs in the _handle_char() function,

9.1 **CVE-2025-51567** Jayesh online exam system

A SQL Injection was found in the /exam/user/profile.php page of kashipara Online Exam System V1.0, which allows remote attackers to execute arbitrary SQL command to get unauthorized database access via the rname, rcollage, rnumber, rgender and rpassword parame

9.8 **CVE-2026-22213** Riot-Os riot

RIOT OS versions up to and including 2026.01-devel-317 contain a stack-based buffer overflow vulnerability in the tapslip6 utility. The vulnerability is caused by unsafe string concatenation in the devopen() function, which constructs a device path using unbou

9.8 **CVE-2025-65552** D3dsecurity zx-g12 firmware

D3D Wi-Fi Home Security System ZX-G12 v2.1.1 is vulnerable to RF replay attacks on the 433 MHz sensor communication channel. The system does not implement rolling codes, message authentication, or anti-replay protection, allowing an attacker within RF range to

9.8 **CVE-2025-67147**

Multiple SQL Injection vulnerabilities exist in amansuryawanshi Gym-Management-System-PHP 1.0 via the 'name', 'email', and 'comment' parameters in (1) submit_contact.php, the 'username' and 'pass_key' parameters in (2) secure_login.php, and the 'login_id', 'pw

9.6 **CVE-2026-22794** Appsmith appsmith

Appsmith is a platform to build admin panels, internal tools, and dashboards. Prior to 1.93, the server uses the Origin value from the request headers as the email link baseUrl without validation. If an attacker controls the Origin, password reset / email veri

9.6 **CVE-2026-22783** Dfir-Iris iris

Iris is a web collaborative platform that helps incident responders share technical details during investigations. Prior to 2.4.24, the DFIR-IRIS datastore file management system has a vulnerability where mass assignment of the file_local_name field combined w

9.9 **CVE-2025-46066** Automai director

An issue in Automai Director v.25.2.0 allows a remote attacker to escalate privileges

9.3 **CVE-2025-41006**

Imaster's MEMS Events CRM contains an SQL injection vulnerability in ‘phone’ parameter in ‘/memsdemo/login.php’.

9.8 **CVE-2025-69270** Broadcom dx netops spectrum

Information Exposure Through Query Strings in GET Request vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Session Hijacking.This issue affects DX NetOps Spectrum: 24.3.8 and earlier.

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.