Daily brief, Wednesday, December 17, 2025

Dec 16, 7:00 PM to Dec 17, 7:00 PM ET

Generated Nov 9, 2026, 4:08 AM ET

0	3	0	29	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 29 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

10.0 **CVE-2025-20393** Cisco Multiple Products CISA KEV

Cisco Secure Email Gateway, Secure Email, AsyncOS, and Web Manager flaw lets attackers run arbitrary commands as root on the appliance OS.

9.3 **CVE-2025-59374** ASUS Live Update CISA KEV

Supply-chain-compromised ASUS Live Update builds embed malicious code that makes devices meeting specific targeting conditions perform unintended actions.

6.6 **CVE-2025-40602** SonicWall SMA1000 appliance CISA KEV

A missing authorization flaw in SonicWall SMA1000 appliances lets an attacker gain unauthorized access to sensitive data and elevated privileges.

New public exploit code

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

New critical CVEs

29

10.0 **CVE-2025-20393** Cisco Multiple Products KEV EXPLOIT CODE

Cisco Secure Email Gateway, Secure Email, AsyncOS, and Web Manager flaw lets attackers run arbitrary commands as root on the appliance OS.

9.3 **CVE-2025-59374** ASUS Live Update KEV

Supply-chain-compromised ASUS Live Update builds embed malicious code that makes devices meeting specific targeting conditions perform unintended actions.

9.8 **CVE-2025-43428** Apple ipados

A configuration issue was addressed with additional restrictions. This issue is fixed in iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2, visionOS 26.2. Photos in the Hidden Photos Album may be viewed without authentication.

9.8 **CVE-2023-53926** Phpjabbers simple cms

PHPJabbers Simple CMS 5.0 contains a SQL injection vulnerability in the 'column' parameter that allows remote attackers to manipulate database queries. Attackers can inject crafted SQL payloads through the 'column' parameter in the index.php endpoint to potent

9.8 **CVE-2025-43526** Apple safari

This issue was addressed with improved URL validation. This issue is fixed in Safari 26.2, macOS Tahoe 26.2. On a Mac with Lockdown Mode enabled, web content opened via a file URL may be able to use Web APIs that should be restricted.

10.0 **CVE-2025-44005**

An attacker can bypass authorization checks and force a Step CA ACME or SCEP provisioner to create certificates without completing certain protocol authorization checks.

9.1 **CVE-2025-68145** Lfprojects model context protocol servers

In mcp-server-git versions prior to 2025.12.17, when the server is started with the --repository flag to restrict operations to a specific repository path, it did not validate that repo_path arguments in subsequent tool calls were actually within that configur

9.9 **CVE-2025-14700** Craftycontrol crafty controller

An input neutralization vulnerability in the Webhook Template component of Crafty Controller allows a remote, authenticated attacker to perform remote code execution via Server Side Template Injection.

10.0 **CVE-2025-62521** Churchcrm churchcrm

ChurchCRM is an open-source church management system. Prior to version 5.21.0, a pre-authentication remote code execution vulnerability in ChurchCRM's setup wizard allows unauthenticated attackers to inject arbitrary PHP code during the initial installation pr

9.1 **CVE-2025-68109** Churchcrm churchcrm

ChurchCRM is an open-source church management system. In versions prior to 6.5.3, the Database Restore functionality does not validate the content or file extension of uploaded files. As a result, an attacker can upload a web shell file and subsequently upload

9.8 **CVE-2025-67895** Apache apache-airflow-providers-edge3

Edge3 Worker RPC RCE on Airflow 2. This issue affects Apache Airflow Providers Edge3: before 2.0.0 - and only if you installed and configured it on Airflow 2. The Edge3 provider support in Airflow 2 has been always development-only and not officially released,

9.8 **CVE-2023-53922** Tinywebgallery tinywebgallery

TinyWebGallery v2.5 contains a remote code execution vulnerability in the admin upload functionality that allows unauthenticated attackers to upload malicious PHP files. Attackers can upload .phar files with embedded system commands to execute arbitrary code o

9.8 **CVE-2025-66647** Riot-Os riot

RIOT is an open-source microcontroller operating system, designed to match the requirements of Internet of Things (IoT) devices and other embedded devices. A vulnerability was discovered in the IPv6 fragmentation reassembly implementation of RIOT OS v2025.07.

9.8 **CVE-2023-53921** Sitemagic sitemagic cms

SitemagicCMS 4.4.3 contains a remote code execution vulnerability that allows attackers to upload malicious PHP files to the files/images directory. Attackers can upload a .phar file with system command execution payload to compromise the web application and e

9.8 **CVE-2025-67073** Tenda ac10 firmware

A Buffer overflow vulnerability in function fromAdvSetMacMtuWan of bin httpd in Tenda AC10V4.0 V16.03.10.20 allows remote attackers to cause denial of service and possibly code execution by sending a post request with a crafted payload (field `serviceName`) to

9.8 **CVE-2023-53914** Ulicms ulicms

UliCMS 2023.1 contains an authentication bypass vulnerability that allows unauthenticated attackers to create admin users through mass assignment in the UserController. Attackers can send a crafted POST request to the admin index.php endpoint with specific par

9.8 **CVE-2023-53923** Ulicms ulicms

UliCMS 2023.1 contains a privilege escalation vulnerability that allows unauthenticated attackers to create administrative accounts through the UserController endpoint. Attackers can send a crafted POST request to /dist/admin/index.php with specific parameters

9.9 **CVE-2025-67164** Pagekit pagekit

An authenticated arbitrary file upload vulnerability in the /storage/poc.php component of Pagekit CMS v1.0.18 allows attackers to execute arbitrary code via uploading a crafted PHP file.

9.8 **CVE-2022-23851** Netaxis api orchestrator

Netaxis API Orchestrator (APIO) before 0.19.3 allows server side template injection (SSTI).

9.8 **CVE-2025-67165** Pagekit pagekit

An Insecure Direct Object Reference (IDOR) in Pagekit CMS v1.0.18 allows attackers to escalate privileges.

9 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Web Hosting Talk webhostingtalk.com 515,149 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.