Daily brief, Friday, January 16, 2026

Jan 15, 7:00 PM to Jan 16, 7:00 PM ET

Generated Nov 7, 2026, 10:05 PM ET

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

21 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

21

9.8 **CVE-2026-23744** Mcpjam inspector DETECTION

MCPJam inspector is the local-first development platform for MCP servers. Versions 1.4.2 and earlier are vulnerable to remote code execution (RCE) vulnerability, which allows an attacker to send a crafted HTTP request that triggers the installation of an MCP s

9.8 **CVE-2025-60021** Apache brpc

Remote command injection vulnerability in heap profiler builtin service in Apache bRPC ((all versions < 1.15.0)) on all platforms allows attacker to inject remote command. Root Cause: The bRPC heap profiler built-in service (/pprof/heap) does not validate the

9.6 **CVE-2026-23523** Openagentplatform dive

Dive is an open-source MCP Host Desktop Application that enables integration with function-calling LLMs. Prior to 0.13.0, crafted deeplink can install an attacker-controlled MCP server configuration without sufficient user confirmation and can lead to arbitrar

9.8 **CVE-2021-47812** Getgrav grav

GravCMS 1.10.7 contains an unauthenticated vulnerability that allows remote attackers to write arbitrary YAML configuration and execute PHP code through the scheduler endpoint. Attackers can exploit the admin-nonce parameter to inject base64-encoded payloads a

10.0 **CVE-2025-61937** Aveva process optimization

The vulnerability, if exploited, could allow an unauthenticated miscreant to achieve remote code execution under OS system privileges of “taoimr” service, potentially resulting in complete compromise of the model application server.

9.8 **CVE-2025-14237** Canon mf455dw firmware

Buffer overflow in XPS font parse processing on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Seri

9.8 **CVE-2021-47785** Ethersoftware ether mp3 cd burner

Ether MP3 CD Burner 1.3.8 contains a buffer overflow vulnerability in the registration name field that allows remote code execution. Attackers can craft a malicious payload to overwrite SEH handlers and execute a bind shell on port 3110 by exploiting improper

9.8 **CVE-2025-14231** Canon lbp1238 ii firmware

Buffer overflow in print job processing by WSD on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Se

9.8 **CVE-2025-14232** Canon mf455dw firmware

Buffer overflow in XML processing of XPS file in Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Ser

9.8 **CVE-2025-14234** Canon mf455dw firmware

Buffer overflow in CPCA list processing on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Sa

9.8 **CVE-2025-14235** Canon mf656cdw firmware

Buffer overflow in XPS font fpgm data processing on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C

9.8 **CVE-2025-14236** Canon mf455dw firmware

Buffer overflow in Address Book attribute tag processing on Small Office Multifunction Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Series/Sate

9.8 **CVE-2025-14233** Canon lbp1238 ii firmware

Invalid free in CPCA file deletion processing on Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *: Satera LBP670C Ser

9.3 **CVE-2012-10064**

Omni Secure Files plugin versions prior to 0.1.14 contain an arbitrary file upload vulnerability in the bundled plupload example endpoint. The /wp-content/plugins/omni-secure-files/plupload/examples/upload.php handler allows unauthenticated uploads without enf

9.8 **CVE-2025-14894** Livewire-Filemanager filemanager

Livewire Filemanager, commonly used in Laravel applications, contains LivewireFilemanagerComponent.php, which does not perform file type and MIME validation, allowing for RCE through upload of a malicious php file that can then be executed via the /storage/ UR

9.1 **CVE-2021-47811** Grocerycrud grocery crud

Grocery Crud 1.6.4 contains a SQL injection vulnerability in the order_by parameter that allows remote attackers to manipulate database queries. Attackers can inject malicious SQL code through the order_by[] parameter in POST requests to the ajax_list endpoint

9.8 **CVE-2025-62581** Deltaww diaview

+1 more CVEs in the same release

Delta Electronics DIAView has multiple vulnerabilities.

10.0 **CVE-2026-23800**

Incorrect Privilege Assignment vulnerability in Modular DS modular-connector allows Privilege Escalation.This issue affects Modular DS: from 2.5.2 before 2.6.0.

9.8 **CVE-2021-47798**

NoteBurner 2.35 contains a buffer overflow vulnerability in the license code input field that allows attackers to crash the application. Attackers can generate a 6000-byte payload and paste it into the 'Name' and 'Code' fields to trigger an application crash.

9.1 **CVE-2026-23722** Wegia wegia

WeGIA is a Web Manager for Charitable Institutions. Prior to 3.6.2, a Reflected Cross-Site Scripting (XSS) vulnerability was discovered in the WeGIA system, specifically within the html/memorando/insere_despacho.php file. The application fails to properly sani

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.