# Daily brief, Thursday, January 15, 2026

Jan 14, 7:00 PM to Jan 15, 7:00 PM ET

Generated Nov 8, 2026, 11:11 PM ET

| 0 | 0 | 0 | 19 | 0 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

19 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

19

**9.8** **CVE-2021-47753** Phpkf cms

phpKF CMS 3.00 Beta y6 contains an unauthenticated file upload vulnerability that allows remote attackers to execute arbitrary code by bypassing file extension checks. Attackers can upload a PHP file disguised as a PNG, rename it, and execute system commands t

**9.8** **CVE-2025-70892** Phpgurukul cyber cafe management system

Phpgurukul Cyber Cafe Management System v1.0 contains a SQL Injection vulnerability in the user management module. The application fails to properly validate user-supplied input in the username parameter of the add-users.php endpoint.

**9.0** **CVE-2026-23520** Arcane arcane

Arcane provides modern docker management. Prior to 1.13.0, Arcane has a command injection in the updater service. Arcane’s updater service supported lifecycle labels com.getarcaneapp.arcane.lifecycle.pre-update and com.getarcaneapp.arcane.lifecycle.post-update

9.8 **CVE-2025-62193**

Sites running NOAA PMEL Live Access Server (LAS) are vulnerable to remote code execution via specially crafted requests that include PyFerret expressions. By leveraging a SPAWN command, a remote, unauthenticated attacker can execute arbitrary OS commands. Fixe

9.3 **CVE-2026-23746**

Entrust Instant Financial Issuance (IFI) On Premise software (formerly referred to as CardWizard) versions 5.x, prior to 6.10.5, and prior to 6.11.1 contain an insecure .NET Remoting exposure in the SmartCardController service (DCG.SmartCardControllerService.e

9.8 **CVE-2023-7334** Chanjetvip t\+

Changjetong T+ versions up to and including 16.x contain a .NET deserialization vulnerability in an AjaxPro endpoint that can lead to remote code execution. A remote attacker can send a crafted request to /tplus/ajaxpro/Ufida.T.CodeBehind._PriorityLevel,App_Co

9.3 **CVE-2011-10041**

Uploadify WordPress plugin versions up to and including 1.0 contain an arbitrary file upload vulnerability in process_upload.php due to missing file type validation. An unauthenticated remote attacker can upload arbitrary files to the affected WordPress site,

9.8 **CVE-2021-47772** 10-Strike network inventory explorer

10-Strike Network Inventory Explorer Pro 9.31 contains a buffer overflow vulnerability in the text file import functionality that allows remote code execution. Attackers can craft a malicious text file with carefully constructed payload to trigger a reverse sh

9.1 **CVE-2026-22908** Sick tdc-x401gl firmware

Uploading unvalidated container images may allow remote attackers to gain full access to the system, potentially compromising its integrity and confidentiality.

9.8 **CVE-2026-23519** Rustcrypto cmov

RustCrypto CMOV provides conditional move CPU intrinsics which are guaranteed on major platforms to execute in constant-time and not be rewritten as branches by the compiler. Prior to 0.4.4, the thumbv6m-none-eabi (Cortex M0, M0+ and M1) compiler emits non-con

9.8 **CVE-2021-47774**

Kingdia CD Extractor 3.0.2 contains a buffer overflow vulnerability in the registration name field that allows attackers to execute arbitrary code. Attackers can craft a malicious payload exceeding 256 bytes to overwrite Structured Exception Handler and gain r

9.1 **CVE-2025-67647** Svelte adapter-node

SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to 2.49.5, SvelteKit is vulnerable to a server side request forgery (SSRF) and denial of service (DoS) under certain conditions. From 2.44.0 through 2.49.4,

9.9 **CVE-2025-67084** Invoiceplane invoiceplane

File upload vulnerability in InvoicePlane through 1.6.3 allows authenticated attackers to upload arbitrary PHP files into attachments, which can later be executed remotely, leading to Remote Code Execution (RCE).

9.8 **CVE-2021-47819**

ProjeQtOr Project Management 9.1.4 contains a file upload vulnerability that allows guest users to upload malicious PHP files with arbitrary code execution capabilities. Attackers can upload a PHP script through the profile attachment section and execute syste

9.8 **CVE-2025-67079** Agora-Project agora-project

File upload vulnerability in Omnispace Agora Project before 25.10 allowing attackers to execute code through the MSL engine of the Imagick library via crafted PDF file to the file upload and thumbnail functions.

9.9 **CVE-2026-22907** Sick tdc-x401gl firmware

An attacker may gain unauthorized access to the host filesystem, potentially allowing them to read and modify system data.

9.4 **CVE-2025-67822** Mitel mivoice mx-one

A vulnerability in the Provisioning Manager component of Mitel MiVoice MX-ONE 7.3 (7.3.0.0.50) through 7.8 SP1 (7.8.1.0.14) could allow an unauthenticated attacker to conduct an authentication bypass attack due to improper authentication mechanisms. A successf

9.8 **CVE-2021-47781**

Cmder Console Emulator 1.3.18 contains a buffer overflow vulnerability that allows attackers to trigger a denial of service condition through a maliciously crafted .cmd file. Attackers can create a specially constructed .cmd file with repeated characters to ov

9.0 **CVE-2026-1009** Altium altium live

A stored cross-site scripting (XSS) vulnerability exists in the Altium Forum due to missing server-side input sanitization in forum post content. An authenticated attacker can inject arbitrary JavaScript into forum posts, which is stored and executed when othe

## 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.