Daily brief, Tuesday, January 27, 2026

Jan 26, 7:00 PM to Jan 27, 7:00 PM ET

Generated Nov 7, 2026, 8:33 PM ET

0	1	0	42	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 42 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.4 **CVE-2026-24858** Fortinet Multiple Products CISA KEV

An authentication bypass in Fortinet FortiGate, FortiAuthenticator, and FortiToken lets an attacker reach administrative interfaces and sensitive data without valid credentials.

New public exploit code

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

New critical CVEs

42

9.4 **CVE-2026-24858** Fortinet Multiple Products KEV EXPLOIT CODE

An authentication bypass in Fortinet FortiGate, FortiAuthenticator, and FortiToken lets an attacker reach administrative interfaces and sensitive data without valid credentials.

9.9 **CVE-2026-1470** N8n n8n

n8n contains a critical Remote Code Execution (RCE) vulnerability in its workflow Expression evaluation system. Expressions supplied by authenticated users during workflow configuration may be evaluated in an execution context that is not sufficiently isolated

9.8 **CVE-2026-24479** Hustoj hustoj

HUSTOF is an open source online judge based on PHP/C++/MySQL/Linux for ACM/ICPC and NOIP training. Prior to version 26.01.24, the problem_import_qduoj.php and problem_import_hoj.php modules fail to properly sanitize filenames within uploaded ZIP archives. Atta

9.8 **CVE-2025-21589**

An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router may allows a network-based attacker to bypass authentication and take administrative control of the device. This issue affects Session Smart Rout

9.8 **CVE-2026-24770** Infiniflow ragflow

RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In version 0.23.1 and possibly earlier versions, the MinerU parser contains a "Zip Slip" vulnerability, allowing an attacker to overwrite arbitrary files on the server (leading to Remote Co

9.1 **CVE-2025-68670** Neutrinolabs xrdp

xrdp is an open source RDP server. xrdp before v0.10.5 contains an unauthenticated stack-based buffer overflow vulnerability. The issue stems from improper bounds checking when processing user domain information during the connection sequence. If exploited, th

9.8 **CVE-2021-47900**

Gila CMS versions prior to 2.0.0 contain a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands through manipulated HTTP headers. Attackers can inject PHP code in the User-Agent header with shell_exec()

9.8 **CVE-2020-36948**

VestaCP 0.9.8-26 contains a session token vulnerability in the LoginAs module that allows remote attackers to manipulate authentication tokens. Attackers can exploit insufficient token validation to access user accounts and perform unauthorized login requests

9.8 **CVE-2025-69559** Carmelo computer book store

code-projects Computer Book Store 1.0 is vulnerable to File Upload in admin_add.php.

9.8 **CVE-2020-36941** Guelfoweb knockpy

Knockpy 4.1.1 contains a CSV injection vulnerability that allows attackers to inject malicious formulas into CSV reports through unfiltered server headers. Attackers can manipulate server response headers to include spreadsheet formulas that will execute when

9.9 **CVE-2026-22039** Kyverno kyverno

Kyverno is a policy engine designed for cloud native platform engineering teams. Versions prior to 1.16.3 and 1.15.3 have a critical authorization boundary bypass in namespaced Kyverno Policy apiCall. The resolved `urlPath` is executed using the Kyverno admiss

9.8 **CVE-2025-69562** Fabian mobile shop management system

code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /insertmessage.php via the userid parameter.

9.8 **CVE-2025-69563** Fabian mobile shop management system

code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /ExLogin.php via the Password parameter.

9.8 **CVE-2025-69565** Fabian mobile shop management system

code-projects Mobile Shop Management System 1.0 is vulnerable to File Upload in /ExAddProduct.php.

9.1 **CVE-2026-24736** Squidex.Io squidex

Squidex is an open source headless content management system and content management hub. Versions of the application up to and including 7.21.0 allow users to define "Webhooks" as actions within the Rules engine. The url parameter in the webhook configuration

9.8 **CVE-2025-69564** Fabian mobile shop management system

code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /ExAddNewUser.php via the Name, Address, email, UserName, Password, confirm_password, Role, Branch, and Activate parameters.

9.8 **CVE-2021-47901**

Dirsearch 0.4.1 contains a CSV injection vulnerability when using the --csv-report flag that allows attackers to inject formulas through redirected endpoints. Attackers can craft malicious server redirects with comma-separated paths containing Excel formulas t

10.0 **CVE-2025-14988**

A security issue has been identified in ibaPDA that could allow unauthorized actions on the file system under certain conditions. This may impact the confidentiality, integrity, or availability of the system.

9.9 **CVE-2026-24740** Amirraminfar dozzle

Dozzle is a realtime log viewer for docker containers. Prior to version 9.0.3, a flaw in Dozzle's agent-backed shell endpoints allows a user restricted by label filters (for example, `label=env=dev`) to obtain an interactive root shell in out?of?scope containe

10.0 **CVE-2026-24822**

Out-of-bounds Write, Heap-based Buffer Overflow vulnerability in ttttupup wxhelper (src modules). This vulnerability is associated with program files mongoose.C. This issue affects wxhelper: through 3.9.10.19-v1.

22 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

SoundCloud soundcloud.com 29,815,722 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.