Daily brief, Thursday, January 29, 2026

Jan 28, 7:00 PM to Jan 29, 7:00 PM ET

Generated Nov 7, 2026, 8:15 PM ET

0	1	0	11	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 11 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2026-1281** Ivanti Endpoint Manager Mobile (EPMM) CISA KEV DETECTION

An attacker gets arbitrary code execution with elevated privileges on the Ivanti Endpoint Manager Mobile (EPMM) server through code injection.

New public exploit code

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

New critical CVEs

11

9.8 **CVE-2026-1281** Ivanti Endpoint Manager Mobile (EPMM) KEV EXPLOIT CODE DETECTION

An attacker gets arbitrary code execution with elevated privileges on the Ivanti Endpoint Manager Mobile (EPMM) server through code injection.

9.8 **CVE-2020-37012**

Tea LaTex 1.0 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary shell commands through the /api.php endpoint. Attackers can craft a malicious LaTeX payload with shell commands that are executed when proce

9.8 **CVE-2020-37002**

Ajenti 2.1.36 contains a post-authenticated remote command execution vulnerability that allows remote attackers to execute arbitrary commands after successful login. Attackers can leverage the /api/terminal/create endpoint to send a netcat reverse shell payloa

9.8 **CVE-2020-37000**

Free MP3 CD Ripper 2.8 contains a stack buffer overflow vulnerability that allows remote attackers to execute arbitrary code by crafting a malicious WAV file with oversized payload. Attackers can leverage a specially crafted exploit file with shellcode, SEH by

9.8 **CVE-2026-1453**

A missing authentication for critical function vulnerability in KiloView Encoder Series could allow an unauthenticated attacker to create or delete administrator accounts. This vulnerability can grant the attacker full administrative control over the product.

10.0 **CVE-2026-24054** Katacontainers kata containers

Kata Containers is an open source project focusing on a standard implementation of lightweight Virtual Machines (VMs) that perform like containers. In versions prior to 3.26.0, when a container image is malformed or contains no layers, containerd falls back to

9.8 **CVE-2026-1188** Eclipse omr

In the Eclipse OMR port library component since release 0.2.0, an API function to return the textual names of all supported processor features was not accounting for the separator inserted between processor features. If the output buffer supplied to this funct

9.1 **CVE-2026-22806**

vCluster Platform provides a Kubernetes platform for managing virtual clusters, multi-tenancy, and cluster sharing. Prior to versions 4.6.0, 4.5.4, 4.4.2, and 4.3.10, when an access key is created with a limited scope, the scope can be bypassed to access resou

9.8 **CVE-2020-37010**

BearShare Lite 5.2.5 contains a buffer overflow vulnerability in the Advanced Search keywords input that allows attackers to execute arbitrary code. Attackers can craft a specially designed payload to overwrite the EIP register and execute shellcode by pasting

9.8 **CVE-2025-69929** N3uron web user interface

An issue in N3uron Web User Interface v.1.21.7-240207.1047 allows a remote attacker to escalate privileges via the password hashing on the client side using the MD5 algorithm over a predictable string format

9.8 **CVE-2020-36997**

BacklinkSpeed 2.4 contains a buffer overflow vulnerability that allows attackers to corrupt the Structured Exception Handler (SEH) chain through malicious file import. Attackers can craft a specially designed payload file to overwrite SEH addresses, potentiall

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.