Daily brief, Monday, January 26, 2026

Jan 25, 7:00 PM to Jan 26, 7:00 PM ET

Generated Nov 7, 2026, 8:37 PM ET

0	5	0	15	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 newly exploited, 15 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

5

10.0 **CVE-2025-52691** SmarterTools SmarterMail CISA KEV DETECTION

Unauthenticated attacker can upload arbitrary files to any location on the SmarterTools SmarterMail mail server, enabling remote code execution.

9.8 **CVE-2026-24061** GNU InetUtils CISA KEV DETECTION

Remote attacker gets authentication bypass on GNU InetUtils telnetd by setting the USER environment variable to "-f root".

9.3 **CVE-2026-23760** SmarterTools SmarterMail CISA KEV DETECTION

Unauthenticated attackers can reset system administrator passwords in SmarterTools SmarterMail via the force-reset-password API, bypassing authentication.

7.8 **CVE-2026-21509** Microsoft Office CISA KEV

A local unauthorized attacker can bypass a security feature in Microsoft Office by exploiting reliance on untrusted inputs in a security decision.

7.8 **CVE-2018-14634** Linux Kernel CISA KEV

An integer overflow in the Linux kernel create_elf_tables() function lets an unprivileged local user with access to a SUID binary escalate privileges.

New public exploit code

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

New critical CVEs

15

9.8 **CVE-2026-24061** GNU InetUtils KEV EXPLOIT CODE DETECTION

Remote attacker gets authentication bypass on GNU InetUtils telnetd by setting the USER environment variable to "-f root".

9.3 **CVE-2026-23760** SmarterTools SmarterMail KEV EXPLOIT CODE DETECTION

Unauthenticated attackers can reset system administrator passwords in SmarterTools SmarterMail via the force-reset-password API, bypassing authentication.

10.0 **CVE-2025-52691** SmarterTools SmarterMail KEV EXPLOIT CODE DETECTION

Unauthenticated attacker can upload arbitrary files to any location on the SmarterTools SmarterMail mail server, enabling remote code execution.

9.9 **CVE-2016-15057** Apache continuum

** UNSUPPORTED WHEN ASSIGNED ** Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Continuum. This issue affects Apache Continuum: all versions. Attackers with access to the installations REST API can us

9.8 **CVE-2026-22709** Vm2 Project vm2

vm2 is an open source vm/sandbox for Node.js. In vm2 prior to version 3.10.2, `Promise.prototype.then` `Promise.prototype.catch` callback sanitization can be bypassed. This allows attackers to escape the sandbox and run arbitrary code. In lib/setup-sandbox.js,

9.3 **CVE-2025-59090**

On the exos 9300 server, a SOAP API is reachable on port 8002. This API does not require any authentication prior to sending requests. Therefore, network access to the exos server allows e.g. the creation of arbitrary access log events as well as querying the

9.3 **CVE-2025-59091**

Multiple hardcoded credentials have been identified, which are allowed to sign-in to the exos 9300 datapoint server running on port 1004 and 1005. This server is used for relaying status information from and to the Access Managers. This information, among othe

9.3 **CVE-2025-59097**

The exos 9300 application can be used to configure Access Managers (e.g. 92xx, 9230 and 9290). The configuration is done in a graphical user interface on the dormakaba exos server. As soon as the save button is clicked in exos 9300, the whole configuration is

9.1 **CVE-2026-24400** Assertj assertj

AssertJ provides Fluent testing assertions for Java and the Java Virtual Machine (JVM). Starting in version 1.4.0 and prior to version 3.27.7, an XML External Entity (XXE) vulnerability exists in `org.assertj.core.util.xml.XmlStringPrettyFormatter`: the `toXml

9.8 **CVE-2026-24436** Tenda w30e firmware

Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) do not enforce rate limiting or account lockout mechanisms on authentication endpoints. This allows attackers to perform unrestricted brute-force attempts against administrative cre

9.2 **CVE-2025-59108**

By default, the password for the Access Manager's web interface, is set to 'admin'. In the tested version changing the password was not enforced.

9.2 **CVE-2025-59103**

The Access Manager 92xx in hardware revision K7 is based on Linux instead of Windows CE embedded in older hardware revisions. In this new hardware revision it was noticed that an SSH service is exposed on port 22. By analyzing the firmware of the devices, it w

9.8 **CVE-2026-24429** Tenda w30e firmware

Shenzhen Tenda W30E V2 firmware versions up to and including V16.01.0.19(5037) ship with a predefined default password for a built-in authentication account that is not required to be changed during initial configuration. An attacker can leverage these default

9.9 **CVE-2025-70982** Bladex springblade

Incorrect access control in the importUser function of SpringBlade v4.5.0 allows attackers with low-level privileges to arbitrarily import sensitive user data.

9.3 **CVE-2026-22696**

dcap-qvl implements the quote verification logic for DCAP (Data Center Attestation Primitives). A vulnerability present in versions prior to 0.3.9 involves a critical gap in the cryptographic verification process within the dcap-qvl. The library fetches QE Ide

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.