Daily brief, Tuesday, March 3, 2026

Mar 2, 7:00 PM to Mar 3, 7:00 PM ET

Generated Nov 7, 2026, 2:52 PM ET

0	2	0	33	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 33 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

8.1 **CVE-2026-22719** Broadcom VMware Aria Operations CISA KEV

Unauthenticated attackers can run arbitrary commands, leading to remote code execution in VMware Aria Operations during support-assisted product migration.

7.8 **CVE-2026-21385** Qualcomm Multiple Chipsets CISA KEV

Multiple Qualcomm chipsets contain a memory corruption flaw triggered during memory allocation using alignments, which lets an attacker corrupt memory.

New public exploit code

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

New critical CVEs

33

10.0 **CVE-2026-24898** Openemr openemr EXPLOIT CODE DETECTION

Affected: OpenEMR prior to version 8.0.0. Attacker gains: Unauthenticated MedEx API tokens. Recommended action: Update OpenEMR to version 8.0.0 or later.

9.8 **CVE-2026-3136** Google cloud build

An improper authorization vulnerability in GitHub Trigger Comment Control in Google Cloud Build prior to 2026-1-26 allows a remote attacker to execute arbitrary code in the build environment. This vulnerability was patched on 26 January 2026, and no customer a

10.0 **CVE-2026-28289** Freescout freescout

FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. A patch bypass vulnerability for CVE-2026-27636 in FreeScout 1.8.206 and earlier allows any authenticated user with file upload permissions to achieve Remote Code Execution (RCE

9.8 **CVE-2026-1492** DETECTION

The User Registration & Membership – Custom Registration Form Builder, Custom Login Form, User Profile, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to improper privilege management in all versions up to, and including, 5.1.2. Thi

9.9 **CVE-2026-24848** Open-Emr openemr

OpenEMR is a free and open source electronic health records and medical practice management application. In 7.0.4 and earlier, the disposeDocument() method in EtherFaxActions.php allows authenticated users to write arbitrary content to arbitrary locations on t

9.8 **CVE-2026-27971** Qwik qwik DETECTION

Qwik is a performance focused javascript framework. qwik <=1.19.0 is vulnerable to RCE due to an unsafe deserialization vulnerability in the server$ RPC mechanism that allows any unauthenticated user to execute arbitrary code on the server with a single HTTP r

9.8 **CVE-2026-3485** Dlink dir-868l firmware DETECTION

A flaw has been found in D-Link DIR-868L 110b03. This affects the function sub_1BF84 of the component SSDP Service. This manipulation of the argument ST causes os command injection. It is possible to initiate the attack remotely. The exploit has been published

9.8 **CVE-2024-55020** Weintek easyweb

A command injection vulnerability in the DHCP activation feature of Weintek cMT-3072XH2 easyweb Web Version v2.1.53, OS v20231011 allows attackers to execute arbitrary commands with root privileges.

9.8 **CVE-2025-59059** Apache ranger

Remote Code Execution Vulnerability in NashornScriptEngineCreator is reported in Apache Ranger versions <= 2.7.0. Users are recommended to upgrade to version 2.8.0, which fixes this issue.

9.8 **CVE-2026-2628**

The All-in-One Microsoft 365 & Entra ID / Azure AD SSO Login plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.2.5. This makes it possible for unauthenticated attackers to bypass authentication and log in as ot

9.1 **CVE-2026-26279** Froxlor froxlor

Froxlor is open source server administration software. Prior to 2.3.4, a typo in Froxlor's input validation code (== instead of =) completely disables email format checking for all settings fields declared as email type. This allows an authenticated admin to s

9.8 **CVE-2025-70240** Dlink dir-513 firmware

Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWAN_Wizard51.

9.8 **CVE-2025-70237** Dlink dir-513 firmware

Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetPortTr.

9.8 **CVE-2025-70234** Dlink dir-513 firmware
Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetQoS.

9.8 **CVE-2025-70239** Dlink dir-513 firmware
Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWAN_Wizard55.

9.8 **CVE-2026-22891** Libbiosig Project libbiosig
A heap-based buffer overflow vulnerability exists in the Intan CLP parsing functionality of The Biosig Project libbiosig 3.9.2 and Master Branch (db9a9a63). A specially crafted Intan CLP file can lead to arbitrary code execution. An attacker can provide a mali

9.8 **CVE-2025-70236** Dlink dir-513 firmware
Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetDomainFilter.

9.8 **CVE-2025-70241** Dlink dir-513 firmware
Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWANType_Wizard5.

9.1 **CVE-2025-66945** Zdir zdir
A path traversal vulnerability exists in the ZIP extraction API of Zdir Pro 4.x. When a crafted ZIP archive is processed by the backend at /api/extract, files may be written outside the intended directory, leading to arbitrary file overwrite and potentially re

9.8 **CVE-2026-3204** Devolutions devolutions server
Improper input validation in the error message page in Devolutions Server 2025.3.16 and earlier allows remote attackers to spoof the displayed error message via a specially crafted URL.

13 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Provecho provecho.bio 712,904 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.