Daily brief, Tuesday, February 3, 2026

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

Generated Nov 7, 2026, 7:27 PM ET

0	4	0	45	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 45 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

9.8 **CVE-2025-40551** SolarWinds Web Help Desk CISA KEV DETECTION

Unauthenticated remote code execution in SolarWinds Web Help Desk via deserialization of untrusted data lets an attacker run commands on the host.

9.8 **CVE-2019-19006** Sangoma FreePBX CISA KEV

Improper authentication in Sangoma FreePBX lets unauthorized users bypass password authentication and access services provided by the FreePBX admin.

8.6 **CVE-2025-64328** Sangoma FreePBX CISA KEV DETECTION

Sangoma FreePBX Endpoint Manager OS command injection lets an authenticated user run OS commands through the testconnection check_ssh_connect() function.

6.8 **CVE-2021-39935** GitLab Community and Enterprise Editions CISA KEV

Server-side request forgery in GitLab Community and Enterprise Editions gives an attacker access to internal systems and services.

New public exploit code

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

New critical CVEs

45

9.8 **CVE-2025-40551** SolarWinds Web Help Desk KEV EXPLOIT CODE DETECTION

Unauthenticated remote code execution in SolarWinds Web Help Desk via deserialization of untrusted data lets an attacker run commands on the host.

9.8 **CVE-2019-19006** Sangoma FreePBX KEV

Improper authentication in Sangoma FreePBX lets unauthorized users bypass password authentication and access services provided by the FreePBX admin.

9.8 **CVE-2025-69971** Frangoteam fuxa DETECTION

FUXA v1.2.7 contains a hard-coded credential vulnerability in server/api/jwt-helper.js. The application uses a hard-coded secret key to sign and verify JWT Tokens. This allows remote attackers to forge valid admin tokens and bypass authentication to gain full

9.8 **CVE-2020-37090** Arox school erp pro

School ERP Pro 1.0 contains a file upload vulnerability that allows students to upload arbitrary PHP files to the messaging system. Attackers can upload malicious PHP scripts through the message attachment feature, enabling remote code execution on the server.

9.9 **CVE-2026-25510** Ci4-Cms-Erp ci4ms

CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.28.5.0, an authenticated user with file editor permissions can achieve Remote Code Execution (RCE)

9.8 **CVE-2026-24936** Asustor data master

When a specific function is enabled while joining a AD Domain from ADM, an improper input parameters validation vulnerability in a specific CGI program allowing an unauthenticated remote attacker to write arbitrary data to any file on the system. By exploiting

9.8 **CVE-2025-67186** Totolink a950rg firmware

TOTOLINK A950RG V4.1.2cu.5204_B20210112 contains a buffer overflow vulnerability in the setUrlFilterRules interface of /lib/cste_modules/firewall.so. The vulnerability occurs because the `url` parameter is not properly validated for length, allowing remote att

9.8 **CVE-2025-69981** Frangoteam fuxa

FUXA v1.2.7 contains an Unrestricted File Upload vulnerability in the `/api/upload` API endpoint. The endpoint lacks authentication mechanisms, allowing unauthenticated remote attackers to upload arbitrary files. This can be exploited to overwrite critical sys

9.8 **CVE-2026-24465** Elecom wab-s300iw-pd firmware

Stack-based buffer overflow vulnerability exists in ELECOM wireless LAN access point devices. A crafted packet may lead to arbitrary code execution.

9.8 **CVE-2020-37071**

CraftCMS 3 vCard Plugin 1.0.0 contains a deserialization vulnerability that allows unauthenticated attackers to execute arbitrary PHP code through a crafted payload. Attackers can generate a malicious serialized payload that triggers remote code execution by e

9.8 **CVE-2025-63624** Sdkede iot smart water meter firmware

SQL Injection vulnerability in Shandong Kede Electronics Co., Ltd IoT smart water meter monitoring platform v.1.0 allows a remote attacker to execute arbitrary code via the imei_list.aspx file.

9.3 **CVE-2026-25150** Qwik qwik

Qwik is a performance focused javascript framework. Prior to version 1.19.0, a prototype pollution vulnerability exists in the formToObj() function within @builder.io/qwik-city middleware. The function processes form field names with dot notation (e.g., user.n

9.8 **CVE-2020-37068** Konicaminolta ftp utility

Konica Minolta FTP Utility 1.0 contains a buffer overflow vulnerability in the LIST command that allows attackers to overwrite system registers. Attackers can send an oversized buffer of 1500 'A' characters to crash the FTP server and potentially execute unaut

9.8 **CVE-2020-37069** Konicaminolta ftp utility

Konica Minolta FTP Utility 1.0 contains a buffer overflow vulnerability in the NLST command that allows attackers to overwrite system registers. Attackers can send an oversized buffer of 1500 'A' characters to crash the FTP server and potentially execute unaut

9.8 **CVE-2025-67188** Totolink a950rg firmware

A buffer overflow vulnerability exists in TOTOLINK A950RG V4.1.2cu.5204_B20210112. The issue resides in the setRadvdCfg interface of the /lib/cste_modules/ipv6.so module. The function fails to properly validate the length of the user-controlled radvdinterfacen

10.0 **CVE-2025-10878** Omran fikir odalari adminpando

A SQL injection vulnerability exists in the login functionality of Fikir Odalari AdminPando 1.0.1 before 2026-01-26. The username and password parameters are vulnerable to SQL injection, allowing unauthenticated attackers to bypass authentication completely. S

9.8 **CVE-2025-61506** Mediacrush mediacrush

An issue was discovered in MediaCrush thru 1.0.1 allowing remote unauthenticated attackers to upload arbitrary files of any size to the /upload endpoint.

9.8 **CVE-2025-57529** Youdatasum cpas audit management system

YouDataSum CPAS Audit Management System <=v4.9 is vulnerable to SQL Injection in /cpasList/findArchiveReportByDah due to insufficient input validation. This allows remote unauthenticated attackers to execute arbitrary SQL commands via crafted input to the para

9.8 **CVE-2020-37082** Weberp weberp

webERP 4.15.1 contains an unauthenticated file access vulnerability that allows remote attackers to download database backup files without authentication. Attackers can directly access generated backup files in the companies/weberp/ directory by requesting the

9.3 **CVE-2025-65078**

An untrusted search path vulnerability has been identified in the Embedded Solutions Framework in various Lexmark devices. This vulnerability can be leveraged by an attacker to execute arbitrary code.

25 more critical CVEs in this window: see the dashboard

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.