Daily brief, Thursday, February 12, 2026

Feb 11, 7:00 PM to Feb 12, 7:00 PM ET

Generated Nov 7, 2026, 5:48 PM ET

0	4	0	23	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 23 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

9.8 **CVE-2024-43468** Microsoft Configuration Manager CISA KEV DETECTION

Unauthenticated attackers can send crafted requests to Microsoft Configuration Manager to inject SQL and run commands on the server.

8.1 **CVE-2025-40536** SolarWinds Web Help Desk CISA KEV DETECTION

An unauthenticated attacker can bypass security controls in SolarWinds Web Help Desk to reach certain restricted functionality.

7.8 **CVE-2026-20700** Apple Multiple Products CISA KEV

An attacker with an existing memory write capability gets arbitrary code execution via a buffer overflow in Apple iOS, macOS, tvOS, watchOS, and visionOS.

7.7 **CVE-2025-15556** Notepad++ Notepad++ CISA KEV

Notepad++ WinGUp updater lacks an integrity check, so an attacker who redirects update traffic gets arbitrary code execution via a malicious installer.

New public exploit code

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

New critical CVEs

23

9.8 **CVE-2024-43468** Microsoft Configuration Manager KEV EXPLOIT CODE DETECTION

Unauthenticated attackers can send crafted requests to Microsoft Configuration Manager to inject SQL and run commands on the server.

9.8 **CVE-2026-24895** Php frankenphp

FrankenPHP is a modern application server for PHP. Prior to 1.11.2, FrankenPHP's CGI path splitting logic improperly handles Unicode characters during case conversion. The logic computes the split index (for finding .php) on a lowercased copy of the request pa

9.8 **CVE-2026-25996** Linuxfoundation inspektor gadget

Inspektor Gadget is a set of tools and framework for data collection and system inspection on Kubernetes clusters and Linux hosts using eBPF. String fields from eBPF events in columns output mode are rendered to the terminal without any sanitization of control

10.0 **CVE-2026-26216** Kidocode crawl4ai DETECTION

Crawl4AI versions prior to 0.8.0 contain a remote code execution vulnerability in the Docker API deployment. The /crawl endpoint accepts a hooks parameter containing Python code that is executed using exec(). The __import__ builtin was included in the allowed

9.9 **CVE-2026-26068** Jm33-M0 emp3r0r

emp3r0r is a stealth-focused C2 designed by Linux users for Linux environments. Prior to 3.21.1, untrusted agent metadata (Transport, Hostname) is accepted during check-in and later interpolated into tmux shell command strings executed via /bin/sh -c. This ena

9.8 **CVE-2026-1358**

Airleader Master versions 6.381 and prior allow for file uploads without restriction to multiple webpages running maximum privileges. This could allow an unauthenticated user to potentially obtain remote code execution on the server.

9.1 **CVE-2026-25227** Goauthentik authentik

authentik is an open-source identity provider. From 2021.3.1 to before 2025.8.6, 2025.10.4, and 2025.12.4, when using delegated permissions, a User that has the permission Can view * Property Mapping or Can view Expression Policy is able to execute arbitrary c

9.8 **CVE-2019-25321** Internet-Soft ftp navigator

FTP Navigator 8.03 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload that triggers a buffer overflow when pasted into the

9.8 **CVE-2026-1729**

The AdForest theme for WordPress is vulnerable to authentication bypass in all versions up to, and including, 6.0.12. This is due to the plugin not properly verifying a user's identity prior to authenticating them through the 'sb_login_user_with_otp_fun' funct

9.8 **CVE-2026-26011** Opennav nav2

navigation2 is a ROS 2 Navigation Framework and System. In 1.3.11 and earlier, a critical heap out-of-bounds write vulnerability exists in Nav2 AMCL's particle filter clustering logic. By publishing a single crafted geometry_msgs/PoseWithCovarianceStamped mess

9.8 **CVE-2019-25319**

Domain Quester Pro 6.02 contains a stack overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the 'Domain Name Keywords' inp

9.8 **CVE-2019-25327**

Prime95 version 29.8 build 6 contains a buffer overflow vulnerability in the user ID input field that allows remote attackers to execute arbitrary code. Attackers can craft a malicious payload and paste it into the PrimeNet user ID and proxy host fields to tri

9.8 **CVE-2025-70314** Ourway webfsd

webfsd 1.21 is vulnerable to a Buffer Overflow via a crafted request. This is due to the filename variable

9.8 **CVE-2019-25337**

OwnCloud 8.1.8 contains a username enumeration vulnerability that allows remote attackers to discover user accounts by manipulating the share.php endpoint. Attackers can send crafted GET requests to /index.php/core/ajax/share.php with a wildcard search paramet

9.8 **CVE-2025-14014**

Unrestricted Upload of File with Dangerous Type vulnerability in NTN Information Processing Services Computer Software Hardware Industry and Trade Ltd. Co. Smart Panel allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Smart Pa

9.8 **CVE-2026-26218** Newbee-Mall Project newbee-mall

newbee-mall includes pre-seeded administrator accounts in its database initialization script. These accounts are provisioned with a predictable default password. Deployments that initialize or reset the database using the provided schema and fail to change the

9.8 **CVE-2025-14892**

The Prime Listing Manager WordPress plugin through 1.1 allows an attacker to gain administrative access without having any kind of account on the targeted site and perform unauthorized actions due to a hardcoded secret.

9.8 **CVE-2025-10969** Farktor e-commerce package

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Farktor Software E-Commerce Services Inc. E-Commerce Package allows Blind SQL Injection. This issue affects E-Commerce Package: through 27112025.

9.8 **CVE-2025-70981** Fit2cloud cordys crm

CordysCRM 1.4.1 is vulnerable to SQL Injection in the employee list query interface (/user/list) via the departmentIds parameter.

9.2 **CVE-2026-24044**

Element Server Suite Community Edition (ESS Community) deploys a Matrix stack using the provided Helm charts and Kubernetes distribution. The ESS Community Helm Chart secrets initialization hook (using matrix-tools container before 0.5.7) is using an insecure

3 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.