Daily brief, Friday, March 6, 2026

Mar 5, 7:00 PM to Mar 6, 7:00 PM ET

Generated Nov 7, 2026, 2:22 PM ET

0	0	0	25	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

25 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

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

New critical CVEs

25

9.8 **CVE-2026-29058** Wwbn avideo-encoder DETECTION

AVideo is a video-sharing Platform software. Prior to version 7.0, an unauthenticated attacker can execute arbitrary OS commands on the server by injecting shell command substitution into the base64Url GET parameter. This can lead to full server compromise, da

9.8 **CVE-2026-29042** Iguazio nuclio

Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. Prior to version 1.15.20, the Nuclio Shell Runtime component contains a command injection vulnerability in how it processes user-supplied arguments. When a function is invoked via HTT

9.8 **CVE-2026-28501** Wwbn avideo

WWBN AVideo is an open source video platform. Prior to version 24.0, an unauthenticated SQL Injection vulnerability exists in AVideo within the objects/videos.json.php and objects/video.php components. The application fails to properly sanitize the catName par

9.8 **CVE-2026-28794** Orpc orpc

oRPC is an tool that helps build APIs that are end-to-end type-safe and adhere to OpenAPI standards. Prior to version 1.13.6, a prototype pollution vulnerability exists in the RPC JSON deserializer of the @orpc/client package. The vulnerability allows unauthen

9.4 **CVE-2026-22552** Epower epower.ie

WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discove

9.8 **CVE-2026-2331**

An attacker may perform unauthenticated read and write operations on sensitive filesystem areas via the AppEngine Fileaccess over HTTP due to improper access restrictions. A critical filesystem directory was unintentionally exposed through the HTTP-based file

9.4 **CVE-2026-26051** Mvm mobiliti e-mobi.hu

WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discove

9.4 **CVE-2026-2330**

An attacker may access restricted filesystem areas on the device via the CROWN REST interface due to incomplete whitelist enforcement. Certain directories intended for internal testing were not covered by the whitelist and are accessible without authentication

9.3 **CVE-2026-29183** B3log siyuan DETECTION

SiYuan is a personal knowledge management system. Prior to version 3.5.9, an unauthenticated reflected XSS vulnerability exists in the dynamic icon API endpoint "GET /api/icon/getDynamicIcon" when type=8, attacker-controlled content is embedded into SVG output

9.4 **CVE-2026-26288** Everon api.everon.io

WebSocket endpoints lack proper authentication mechanisms, enabling attackers to perform unauthorized station impersonation and manipulate data sent to the backend. An unauthenticated attacker can connect to the OCPP WebSocket endpoint using a known or discove

9.1 **CVE-2026-29065** Webtechnologies changedetection

changedetection.io is a free open source web page change detection tool. Prior to version 0.54.4, a Zip Slip vulnerability in the backup restore functionality allows arbitrary file overwrite via path traversal in uploaded ZIP archives. This issue has been patc

9.8 **CVE-2026-27005** Depomo chartbrew

Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to version 4.8.3, an unauthenticated attacker can inject arbitrary SQL into queries executed against databases connected to Cha

9.8 **CVE-2026-28514** Rocket.Chat rocket.chat

Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to versions 7.8.6, 7.9.8, 7.10.7, 7.11.4, 7.12.4, 7.13.3, and 8.0.0, a critical authentication bypass vulnerability exists in Rocket.Chat's account service used in the ddp

9.8 **CVE-2026-28802** Authlib authlib

Authlib is a Python library which builds OAuth and OpenID Connect servers. From version 1.6.5 to before version 1.6.7, previous tests involving passing a malicious JWT containing alg: none and an empty signature was passing the signature verification step with

9.1 **CVE-2026-28497** Ritlabs tinyweb

TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. Prior to version 2.03, an integer overflow vulnerability in the string-to-integer conversion routine (_Val) allows an unauthenticated remote attacker to bypass Content-Length restrictions and p

9.8 **CVE-2026-28795** Zhongyu09 openchatbi

OpenChatBI is an intelligent chat-based BI tool powered by large language models, designed to help users query, analyze, and visualize data through natural language conversations. Prior to version 0.2.2, the save_report tool in openchatbi/tool/save_report.py s

9.8 **CVE-2026-28710** Acronis cyber protect

Sensitive information disclosure and manipulation due to improper authentication. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 41186.

9.8 **CVE-2026-2446**

The PowerPack for LearnDash WordPress plugin before 1.3.0 does not have authorization and CRSF checks in an AJAX action, allowing unauthenticated users to update arbitrary WordPress options (such as default_role etc) and create arbitrary admin users

9.9 **CVE-2026-29789** Vitodeploy vito

Vito is a self-hosted web application that helps manage servers and deploy PHP applications into production servers. Prior to version 3.20.3, a missing authorization check in workflow site-creation actions allows an authenticated attacker with workflow write a

9.8 **CVE-2026-28785** Ghostfol ghostfolio

Ghostfolio is an open source wealth management software. Prior to version 2.244.0, by bypassing symbol validation, an attacker can execute arbitrary SQL commands via the getHistorical() method, potentially allowing them to read, modify, or delete sensitive fin

5 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.