Daily brief, Wednesday, March 11, 2026

Mar 10, 8:00 PM to Mar 11, 8:00 PM ET

Generated Nov 7, 2026, 1:35 PM ET

0	1	0	39	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 39 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2025-68613** N8n n8n CISA KEV DETECTION

n8n workflow expression evaluation contains a flaw in dynamically managed code resources that lets an attacker achieve remote code execution.

New public exploit code

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

New critical CVEs

39

10.0 **CVE-2025-68613** N8n n8n KEV EXPLOIT CODE DETECTION

n8n workflow expression evaluation contains a flaw in dynamically managed code resources that lets an attacker achieve remote code execution.

9.0 **CVE-2023-27573** Netboxlabs netbox-docker

netbox-docker before 2.5.0 has a superuser account with default credentials (admin password for the admin account, and 0123456789abcdef0123456789abcdef01234567 value for SUPERUSER_API_TOKEN). In practice on the public Internet, almost all users changed the pas

9.8 **CVE-2026-31900** Python black

Black is the uncompromising Python code formatter. Black provides a GitHub action for formatting code. This action supports an option, use_pyproject: true, for reading the version of Black to use from the repository pyproject.toml. A malicious pull request cou

9.6 **CVE-2026-3916** Google chrome

Out of bounds read in Web Speech in Google Chrome prior to 146.0.7680.71 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-30903** Zoom workplace desktop

External Control of File Name or Path in the Mail feature of Zoom Workplace for Windows before 6.6.0 may allow an unauthenticated user to conduct an escalation of privilege via network access.

9.8 **CVE-2019-25487**

SAPIDO RB-1732 V2.0.43 contains a remote command execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious input to the formSysCmd endpoint. Attackers can send POST requests with the sysCmd param

9.8 **CVE-2026-31975** Cloudcli cloud cli

+1 more CVEs in the same release

Cloud CLI (aka Claude Code UI) is a desktop and mobile UI for Claude Code, Cursor CLI, Codex, and Gemini-CLI. Prior to 1.25.0, OS Command Injection via WebSocket Shell. Both projectPath and initialCommand in server/index.js are taken directly from the WebSocke

9.8 **CVE-2019-25471** Leefish file thingie

FileThingie 2.5.7 contains an arbitrary file upload vulnerability that allows attackers to upload malicious files by sending ZIP archives through the ft2.php endpoint. Attackers can upload ZIP files containing PHP shells, use the unzip functionality to extract

9.8 **CVE-2026-30741** Openclaw openclaw

A remote code execution (RCE) vulnerability in OpenClaw Agent Platform v2026.2.6 allows attackers to execute arbitrary code via a Request-Side prompt injection attack.

9.8 **CVE-2019-25468**

NetGain EM Plus 10.1.68 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious parameters to the script_test.jsp endpoint. Attackers can send POST requests with shell co

9.8 **CVE-2026-23813** Hpe arubaos-cx

A vulnerability has been identified in the web-based management interface of AOS-CX switches that could potentially allow an unauthenticated remote actor to circumvent existing authentication controls. In some cases this could enable resetting the admin passwo

9.8 **CVE-2026-32136** Adguard adguardhome

AdGuard Home is a network-wide software for blocking ads and tracking. Prior to 0.107.73, an unauthenticated remote attacker can bypass all authentication in AdGuardHome by sending an HTTP/1.1 request that requests an upgrade to HTTP/2 cleartext (h2c). Once th

9.9 **CVE-2026-27591** Wintercms winter

Winter is a free, open-source content management system (CMS) based on the Laravel PHP framework. Prior to 1.0.477, 1.1.12, and 1.2.12, Winter CMS allowed authenticated backend users to escalate their accounts level of access to the system by modifying the rol

10.0 **CVE-2026-27897** Wanderingastronomer vociferous

Vociferous provides cross-platform, offline speech-to-text with local AI refinement. Prior to 4.4.2, the vulnerability exists in src/api/system.py within the export_file route. The application accepts a JSON payload containing a filename and content. While the

9.8 **CVE-2026-28229** Argoproj argo workflows

Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. Prior to 4.0.2 and 3.7.11, Workflow templates endpoints allow any client to retrieve WorkflowTemplates (and ClusterWorkflowTemplates). Any request

9.8 **CVE-2026-31874** Taskosaur taskosaur

Taskosaur is an open source project management platform with conversational AI for task execution in-app. In 1.0.0, the application does not properly validate or restrict the role parameter during the user registration process. An attacker can manually modify

9.8 **CVE-2026-27842**

Authentication bypass issue exists in MR-GM5L-S1 and MR-GM5A-L1, which may allow an attacker to bypass authentication and change the device configuration.

9.8 **CVE-2026-2631**

The Datalogics Ecommerce Delivery WordPress plugin before 2.6.60 exposes an unauthenticated REST endpoint that allows any remote user to modify the option `datalogics_token` without verification. This token is subsequently used for authentication in a protecte

9.8 **CVE-2025-70024**

An issue pertaining to CWE-89: Improper Neutralization of Special Elements used in an SQL Command was discovered in benkeen generatedata 4.0.14.

9.8 **CVE-2026-3826** Wellchoose organization portal system

IFTOP developed by WellChoose has a Local File Inclusion vulnerability, allowing unauthenticated remote attackers to execute arbitrary code on the server.

18 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.