Daily brief, Monday, March 30, 2026

Mar 29, 8:00 PM to Mar 30, 8:00 PM ET

Generated Nov 7, 2026, 10:09 AM ET

0	1	0	22	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 22 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.3 **CVE-2026-3055** Citrix NetScaler CISA KEV DETECTION

An attacker can read sensitive information from system memory on Citrix NetScaler devices through an out-of-bounds read flaw.

New public exploit code

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

New critical CVEs

22

9.3 **CVE-2026-3055** Citrix NetScaler KEV EXPLOIT CODE DETECTION

An attacker can read sensitive information from system memory on Citrix NetScaler devices through an out-of-bounds read flaw.

9.8 **CVE-2026-33032** Nginxui nginx ui DETECTION

Nginx UI is a web user interface for the Nginx web server. In versions 2.3.5 and prior, the nginx-ui MCP (Model Context Protocol) integration exposes two HTTP endpoints: /mcp and /mcp_message. While /mcp requires both IP whitelisting and authentication (AuthRe

9.1 **CVE-2026-33026** Nginxui nginx ui

Nginx UI is a web user interface for the Nginx web server. Prior to version 2.3.4, the nginx-ui backup restore mechanism allows attackers to tamper with encrypted backup archives and inject malicious configuration during restoration. This issue has been patche

9.8 **CVE-2026-4257** DETECTION

The Contact Form by Supsystic plugin for WordPress is vulnerable to Server-Side Template Injection (SSTI) leading to Remote Code Execution (RCE) in all versions up to, and including, 1.7.36. This is due to the plugin using the Twig `Twig_Loader_String` templat

10.0 **CVE-2025-15379** Lfprojects mlflow

A command injection vulnerability exists in MLflow's model serving container initialization code, specifically in the `_install_model_dependencies_to_env()` function. When deploying a model with `env_manager=LOCAL`, MLflow reads dependency specifications from

9.8 **CVE-2026-30305** Orangecat syntx

Syntx's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on fragile regular expressions to parse command structures; while it attempts to

9.8 **CVE-2026-30307** Roocode roo code

Roo Code's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on fragile regular expressions to parse command structures; while it attempts

9.8 **CVE-2026-30313** Cline cline

DSAI-Cline's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on string-based parsing to validate commands; while it intercepts dangerous

9.8 **CVE-2026-2287** Crewai crewai

CrewAI does not properly check that Docker is still running during runtime, and will fall back to a sandbox setting that allows for RCE exploitation.

9.8 **CVE-2026-4789** Kyverno kyverno

Kyverno, versions 1.16.0 and later, are vulnerable to SSRF due to unrestricted CEL HTTP functions.

9.8 **CVE-2026-30306** Rahmanazhar sakadev

In its design for automatic terminal command execution, SakaDev offers two options: Execute safe commands and execute all commands. The description for the former states that commands determined by the model to be safe will be automatically executed, whereas i

9.2 **CVE-2026-34714** Vim vim

Vim before 9.2.0272 allows code execution that happens immediately upon opening a crafted file in the default configuration, because %{expr} injection occurs with tabpanel lacking P_MLE.

10.0 **CVE-2025-15036** Lfprojects mlflow

A path traversal vulnerability exists in the `extract_archive_to_dir` function within the `mlflow/pyfunc/dbconnect_artifact_cache.py` file of the mlflow/mlflow repository. This vulnerability, present in versions before v3.7.0, arises due to the lack of validat

9.8 **CVE-2026-30308** Presidio hai build

In its design for automatic terminal command execution, HAI Build Code Generator offers two options: Execute safe commands and Execute all commands. The description for the former states that commands determined by the model to be safe will be automatically ex

9.8 **CVE-2026-2286** Crewai crewai

CrewAI contains a server-side request forgery vulnerability that enables content acquisition from internal and cloud services, facilitated by the RAG search tools not properly validating URLs provided at runtime.

10.0 **CVE-2026-28505** Tautulli tautulli

Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Prior to version 2.17.0, the str_eval() function in notification_handler.py implements a sandboxed eval() for notification text templates. The sandbox attempts to restrict callable

9.6 **CVE-2026-2275**

The CrewAI CodeInterpreter tool falls back to SandboxPython when it cannot reach Docker, which can enable RCE through arbitrary C function calling.

9.1 **CVE-2026-32275** Tautulli tautulli

Tautulli is a Python based monitoring and tracking tool for Plex Media Server. From version 1.3.10 to before version 2.17.0, an unsanitized JSONP callback parameter allows cross-origin script injection and API key theft. This issue has been patched in version

9.3 **CVE-2026-30562** Ahsanriaz26gmailcom sales and inventory system

A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_stock.php file via the "msg" parameter. The application fails to sanitize the input, allowing remote attackers

9.1 **CVE-2026-34557** Ci4-Cms-Erp ci4ms

+1 more CVEs in the same release

CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within group and role mana

1 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.