Daily brief, Tuesday, March 10, 2026

Mar 9, 8:00 PM to Mar 10, 8:00 PM ET

Generated Nov 8, 2026, 2:12 PM ET

0	0	0	36	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

36 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

36

9.8 **CVE-2026-23240** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: tls: Fix race condition in tls_sw_cancel_work_tx() This issue was discovered during a code audit. After cancel_delayed_work_sync() is called from tls_sk_proto_close(), tx_work_handler() can st

9.8 **CVE-2026-0110** Google android

In MM_DATA_IND of cn_NrSmMsgHdlrFromMM.cpp, there is a possible EoP due to memory corruption. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

9.8 **CVE-2026-0111** Google android

+1 more CVEs in the same release

In ns_GetUserData of ns_SmscbUtilities.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitatio

9.8 **CVE-2026-0114** Google android

+1 more CVEs in the same release

In Modem, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

9.8 **CVE-2026-0116** Google android

In __mfc_handle_released_buf of mfc_core_isr.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

10.0 **CVE-2025-48611** Google android

In DeviceId of DeviceId.java, there is a possible desync in persistence due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

9.0 **CVE-2026-27825** Mcp-Atlassian mcp atlassian

MCP Atlassian is a Model Context Protocol (MCP) server for Atlassian products (Confluence and Jira). Prior to version 0.17.0, the `confluence_download_attachment` MCP tool accepts a `download_path` parameter that is written to without any directory boundary en

9.8 **CVE-2025-41709**

An unauthenticated remote attacker can perform a command injection via Modbus-TCP or Modbus-RTU to gain read and write access on the affected device.

10.0 **CVE-2026-30965** Parseplatform parse-server DETECTION

+2 more CVEs in the same release

Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.5.2-alpha.8 and 8.6.21, a vulnerability in Parse Server's query handling allows an authenticated or unauthenticated attacker to exfiltrate sessio

9.8 **CVE-2026-28292** Simple-Git Project simple-git

`simple-git`, an interface for running git commands in any node.js application, has an issue in versions 3.15.0 through 3.32.2 that allows an attacker to bypass two prior CVE fixes (CVE-2022-25860 and CVE-2022-25912) and achieve full remote code execution on t

9.9 **CVE-2026-30957** Hackerbay oneuptime

OneUptime is a solution for monitoring and managing online services. Prior to 10.0.21, OneUptime Synthetic Monitors allow a low-privileged authenticated project user to execute arbitrary commands on the oneuptime-probe server/container. The root cause is that

9.3 **CVE-2026-30869** B3log siyuan

SiYuan is a personal knowledge management system. Prior to 3.5.10, a path traversal vulnerability in the /export endpoint allows an attacker to read arbitrary files from the server filesystem. By exploiting double?encoded traversal sequences, an attacker can a

9.8 **CVE-2025-56422** Limesurvey limesurvey

A deserialization vulnerability in LimeSurvey before v6.15.0+250623 allows a remote attacker to execute arbitrary code on the server.

9.8 **CVE-2026-3843** Bukts buk ts-g gas station automation system

Nefteprodukttekhnika BUK TS-G Gas Station Automation System 2.9.1 on Linux contains a SQL Injection vulnerability (CWE-89) in the system configuration module. A remote attacker can send specially crafted HTTP POST requests to the /php/request.php endpoint via

9.8 **CVE-2026-0953**

The Tutor LMS Pro plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 3.9.5 via the Social Login addon. This is due to the plugin failing to verify that the email provided in the authentication request matches the

9.1 **CVE-2026-27685**

SAP NetWeaver Enterprise Portal Administration is vulnerable if a privileged user uploads untrusted or malicious content that, upon deserialization, could result in a high impact on the confidentiality, integrity, and availability of the host system.

9.8 **CVE-2026-29792** Feathersjs feathers

+1 more CVEs in the same release

Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. From 5.0.0 to before 5.0.42, an unauthenticated attacker can send a crafted GET request directly to /oauth/:provider/callback with a forged profile in the

9.6 **CVE-2025-40943**

Affected devices do not properly sanitize contents of trace files. This could allow an attacker to inject code through social engineering an authorized user, who has the function right "Read diagnostics", to import a specially crafted trace file. The malicious

9.9 **CVE-2026-30956** Hackerbay oneuptime

OneUptime is a solution for monitoring and managing online services. Prior to 10.0.21, a low?privileged user can bypass authorization and tenant isolation in OneUptime v10.0.20 and earlier by sending a forged is-multi-tenant-query header together with a contro

9.1 **CVE-2025-69615** Telekom account management portal

Incorrect Access Control via missing 2FA rate-limiting allowing unlimited brute-force retries and full MFA bypass with no user interaction required. Affected Product: Deutsche Telekom AG Telekom Account Management Portal, versions before 2025-10-24, fixed 2025

11 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.