Daily brief, Monday, March 9, 2026

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

Generated Nov 7, 2026, 1:56 PM ET

0	3	0	13	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 newly exploited, 13 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

9.8 **CVE-2025-26399** SolarWinds Web Help Desk CISA KEV DETECTION

An attacker can run commands on the host running SolarWinds Web Help Desk by exploiting a deserialization of untrusted data flaw in its AjaxProxy component.

8.6 **CVE-2026-1603** Ivanti Endpoint Manager (EPM) CISA KEV DETECTION

An unauthenticated attacker bypasses authentication to reach the Ivanti Endpoint Manager (EPM) console and, from there, the wider network.

7.5 **CVE-2021-22054** Omnissa Workspace One UEM CISA KEV DETECTION

Omnissa Workspace One UEM formerly known as VMware Workspace One UEM contains a server-side request forgery (SSRF) vulnerability that could allow a malicious actor with network access to UEM to send their requests without authentication and to gain access to s

New public exploit code

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

New critical CVEs

13

9.8 **CVE-2025-26399** SolarWinds Web Help Desk KEV EXPLOIT CODE DETECTION

An attacker can run commands on the host running SolarWinds Web Help Desk by exploiting a deserialization of untrusted data flaw in its AjaxProxy component.

9.1 **CVE-2026-31816** Budibase budibase DETECTION

Budibase is a low code platform for creating internal tools, workflows, and admin panels. In 3.31.4 and earlier, the Budibase server's authorized() middleware that protects every server-side API endpoint can be completely bypassed by appending a webhook path p

9.8 **CVE-2026-3630** Deltaww commgr2

Delta Electronics COMMGR2 has Stack-based Buffer Overflow vulnerability.

9.8 **CVE-2026-3823** Blackbeartechhive atop ehg2408 firmware

EHG2408 series switch developed by Atop Technologies has a Stack-based Buffer Overflow vulnerability, allowing unauthenticated remote attackers to control the program's execution flow and execute arbitrary code.

9.8 **CVE-2026-24713** Apache iotdb

Improper Input Validation vulnerability in Apache IoTDB. This issue affects Apache IoTDB: from 1.0.0 before 1.3.7, from 2.0.0 before 2.0.7. Users are recommended to upgrade to version 1.3.7 or 2.0.7, which fixes the issue.

9.8 **CVE-2026-24015** Apache iotdb

A vulnerability in Apache IoTDB. This issue affects Apache IoTDB: from 1.0.0 before 1.3.7, from 2.0.0 before 2.0.7. Users are recommended to upgrade to version 1.3.7 or 2.0.7, which fixes the issue.

9.1 **CVE-2025-41764** Mbs-Solutions universal bacnet router firmware

Due to insufficient authorization enforcement, an unauthorized remote attacker can exploit the wwwupdate.cgi endpoint to upload and apply arbitrary updates.

9.8 **CVE-2025-70039** Linagora twake

An issue pertaining to CWE-78: Improper Neutralization of Special Elements used in an OS Command was discovered in linagora Twake v2023.Q1.1223.

9.8 **CVE-2025-70046** Miazzy oa-font-service

An issue pertaining to CWE-829: Inclusion of Functionality from Untrusted Control Sphere was discovered in Miazzy oa-front-service master.

9.8 **CVE-2025-70042** Opensourcelabs thermakube

An issue pertaining to CWE-918: Server-Side Request Forgery was discovered in oslabs-beta ThermaKube master.

9.8 **CVE-2025-40639** Sbitsoft eventobot

A SQL injection vulnerability has been found in Eventobot. This vulnerability allows an attacker to retrieve, create, update and delete databases through the 'promo_send' parameter in the '/assets/php/calculate_discount.php'.

9.6 **CVE-2026-30240** Budibase budibase

Budibase is a low code platform for creating internal tools, workflows, and admin panels. In 3.31.5 and earlier, a path traversal vulnerability in the PWA (Progressive Web App) ZIP processing endpoint (POST /api/pwa/process-zip) allows an authenticated user wi

9.1 **CVE-2025-41765** Mbs-Solutions universal bacnet router firmware

Due to insufficient authorization enforcement, an unauthorized remote attacker can exploit the wwwupload.cgi endpoint to upload and apply arbitrary data. This includes, but is not limited to, contact images, HTTPS certificates, system backups for restoration,

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.