# Daily brief, Thursday, March 12, 2026

Mar 11, 8:00 PM to Mar 12, 8:00 PM ET

Generated Nov 7, 2026, 1:24 PM ET

| 0 | 0 | 0 | 21 | 0 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

21 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

21

**9.1** **CVE-2026-21671** Veeam Software Appliance

Product not on watchlist.

**10.0** **CVE-2026-21669** Veeam Backup and Replication

**+2 more CVEs in the same release**

Product not on watchlist.

**9.9** **CVE-2026-21708** Veeam Backup and Replication

Product not on watchlist.

**10.0** **CVE-2026-3611** Honeywell iq4e firmware

The Honeywell IQ4x building management controller, exposes its full web-based HMI without authentication in its factory-default configuration. With no user module configured, security is disabled by design and the system operates under a System Guest (level 10

9.8 **CVE-2026-26792** Gl-Inet ar300m16 firmware

GL-iNet GL-AR300M16 v4.3.11 was discovered to contain multiple command injection vulnerabilities in the set_upgrade function via the modem_url, target_version, current_version, firmware_upload, hash_type, hash_value, and upgrade_type parameters. These vulnerab

9.8 **CVE-2026-26791** Gl-Inet ar300m16 firmware

GL-iNet GL-AR300M16 v4.3.11 was discovered to contain a command injection vulnerability via the string port parameter in the enable_echo_server function. This vulnerability allows attackers to execute arbitrary commands via a crafted input.

9.8 **CVE-2026-26795** Gl-Inet ar300m16 firmware

GL-iNet GL-AR300M16 v4.3.11 was discovered to contain a command injection vulnerability via the module parameter in the M.get_system_log function. This vulnerability allows attackers to execute arbitrary commands via a crafted input.

9.8 **CVE-2026-26793** Gl-Inet ar300m16 firmware

GL-iNet GL-AR300M16 v4.3.11 was discovered to contain a command injection vulnerability via the set_config function. This vulnerability allows attackers to execute arbitrary commands via a crafted input.

9.8 **CVE-2026-3059** Lmsys sglang

SGLang's multimodal generation module is vulnerable to unauthenticated remote code execution through the ZMQ broker, which deserializes untrusted data using pickle.loads() without authentication.

9.8 **CVE-2026-3060** Lmsys sglang

SGLang' encoder parallel disaggregation system is vulnerable to unauthenticated remote code execution through the disaggregation module, which deserializes untrusted data using pickle.loads() without authentication.

9.9 **CVE-2026-28384** Canonical lxd

An improper sanitization of the compression_algorithm parameter in Canonical LXD allows an authenticated, unprivileged user to execute commands as the LXD daemon on the LXD server via API calls to the image and backup endpoints. This issue affected LXD from 4.

9.8 **CVE-2026-32248** Parseplatform parse-server

Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.6.0-alpha.12 and 8.6.38, an unauthenticated attacker can take over any user account that was created with an authentication provider that does no

9.8 **CVE-2026-32232** Aisarlabs zeptoclaw

ZeptoClaw is a personal AI assistant. Prior to 0.7.6, there is a Dangling Symlink Component Bypass, TOCTOU Between Validation and Use, and Hardlink Alias Bypass. This vulnerability is fixed in 0.7.6.

9.8 **CVE-2025-70245** Dlink dir-513 firmware

Stack buffer overflow vulnerability in D-Link DIR-513 v1.10 via the curTime parameter to goform/formSetWizardSelectMode.

9.6 **CVE-2026-28792** Ssw tinacms\/cli

Tina is a headless content management system. Prior to 2.1.8 , the TinaCMS CLI dev server combines a permissive CORS configuration (Access-Control-Allow-Origin: *) with the path traversal vulnerability (previously reported) to enable a browser-based drive-by a

9.8 **CVE-2025-59388** Qnap hyper data protector

A use of hard-coded password vulnerability has been reported to affect Hyper Data Protector. The remote attackers can then exploit the vulnerability to gain unauthorized access. We have already fixed the vulnerability in the following version: Hyper Data Prote

9.8 **CVE-2026-28255** Trane tracer sc firmware

A Use of Hard-coded Credentials vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to disclose sensitive information and take over accounts.

9.8 **CVE-2026-28256** Trane tracer sc\+ firmware

A Use of Hard-coded, Security-relevant Constants vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to disclose sensitive information and take over accounts.

9.8 **CVE-2026-28252** Trane tracer sc firmware

A Use of a Broken or Risky Cryptographic Algorithm vulnerability in Trane Tracer SC, Tracer SC+, and Tracer Concierge could allow an attacker to bypass authentication and gain root-level access to the device.

## 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.