Daily brief, Monday, March 23, 2026

Mar 22, 8:00 PM to Mar 23, 8:00 PM ET

Generated Nov 7, 2026, 11:07 AM ET

0	0	0	23	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

23 new critical CVEs, 1 new breaches.

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

23

9.4 **CVE-2026-4404** Linuxfoundation harbor

Use of hard coded credentials in GoHarbor Harbor version 2.15.0 and below, allows attackers to use the default password and gain access to the web UI.

10.0 **CVE-2026-33478** Wwbn avideo DETECTION

WWBN AVideo is an open source video platform. In versions up to and including 26.0, multiple vulnerabilities in AVideo's CloneSite plugin chain together to allow a completely unauthenticated attacker to achieve remote code execution. The `clones.json.php` endp

9.8 **CVE-2026-4585**

A vulnerability has been found in Tiandy Easy7 Integrated Management Platform up to 7.17.0. This vulnerability affects unknown code of the file /Easy7/apps/WebService/ImportSystemConfiguration.jsp of the component Configuration Handler. The manipulation of the

9.8 **CVE-2026-4567** Tenda a15 firmware

A vulnerability has been found in Tenda A15 15.13.07.13. The impacted element is the function UploadCfg of the file /cgi-bin/UploadCfg. The manipulation of the argument File leads to stack-based buffer overflow. The attack may be initiated remotely. The exploi

9.8 **CVE-2026-30849** Mantisbt mantisbt DETECTION

Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions prior to 2.28.1 running on MySQL family databases are affected by an authentication bypass vulnerability in the SOAP API, as a result of an improper type checking on the password parameter

9.3 **CVE-2026-4681**

A critical remote code execution (RCE) vulnerability has been reported in PTC Windchill and PTC FlexPLM. The vulnerability may be exploited through the deserialization of untrusted data. This issue affects Windchill PDMLink: 11.0 M030, 11.1 M020, 11.2.1.0, 12.

10.0 **CVE-2026-3587**

An unauthenticated remote attacker can exploit a hidden function in the CLI prompt to escape the restricted interface, leading to full compromise of the device.

9.8 **CVE-2026-32968**

Due to the improper neutralisation of special elements used in an OS command, an unauthenticated remote attacker can exploit an RCE vulnerability in the com_mb24sysapi module, resulting in full system compromise. This vulnerability is a variant attack for CVE-

9.8 **CVE-2026-33352** Wwbn avideo

WWBN AVideo is an open source video platform. Prior to version 26.0, an unauthenticated SQL injection vulnerability exists in `objects/category.php` in the `getAllCategories()` method. The `doNotShowCats` request parameter is sanitized only by stripping single

9.1 **CVE-2026-4599** Kjur jsrsasign

Versions of the package jsrsasign from 7.0.0 and before 11.1.1 are vulnerable to Incomplete Comparison with Missing Factors via the getRandomBigIntegerZeroToMax and getRandomBigIntegerMinToMax functions in src/crypto-1.1.js; an attacker can recover the private

9.3 **CVE-2026-33502** Wwbn avideo

WWBN AVideo is an open source video platform. In versions up to and including 26.0, an unauthenticated server-side request forgery vulnerability in `plugin/Live/test.php` allows any remote user to make the AVideo server send HTTP requests to arbitrary URLs. Th

9.4 **CVE-2026-33716** Wwbn avideo

WWBN AVideo is an open source video platform. In versions up to and including 26.0, the standalone live stream control endpoint at `plugin/Live/standAloneFiles/control.json.php` accepts a user-supplied `streamerURL` parameter that overrides where the server se

9.1 **CVE-2026-33351** Wwbn avideo

WWBN AVideo is an open source video platform. Prior to version 26.0, a Server-Side Request Forgery (SSRF) vulnerability exists in `plugin/Live/standAloneFiles/saveDVR.json.php`. When the AVideo Live plugin is deployed in standalone mode (the intended configura

9.4 **CVE-2026-2298**

Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Salesforce Marketing Cloud Engagement allows Web Services Protocol Manipulation. This issue affects Marketing Cloud Engagement: before January 30th, 2026.

9.1 **CVE-2025-60949** Csprousers csweb

Census CSWeb 8.0.1 allows "app/config" to be reachable via HTTP in some deployments. A remote, unauthenticated attacker could send requests to configuration files and obtain leaked secrets. Fixed in 8.1.0 alpha.

9.1 **CVE-2026-33297** Wwbn avideo

WWBN AVideo is an open source video platform. Prior to version 26.0, the `setPassword.json.php` endpoint in the CustomizeUser plugin allows administrators to set a channel password for any user. Due to a logic error in how the submitted password value is proce

9.8 **CVE-2026-31851** Nexxtsolutions nebula300plus firmware

Nexxt Solutions Nebula 300+ firmware through version 12.01.01.37 does not implement rate limiting or account lockout mechanisms on authentication interfaces. An attacker can perform unlimited authentication attempts against endpoints that rely on credential va

9.0 **CVE-2026-0898**

An arbitrary file-write vulnerability in Pega Browser Extension (PBE) affects Pega Robot Studio developers who are automating Google Chrome and Microsoft Edge using either version 22.1 or R25. This vulnerability does not affect Robot Runtime users. A bad actor

9.3 **CVE-2026-32913** Openclaw openclaw

OpenClaw before 2026.3.7 contains an improper header validation vulnerability in fetchWithSsrFGuard that forwards custom authorization headers across cross-origin redirects. Attackers can trigger redirects to different origins to intercept sensitive headers li

9.8 **CVE-2026-31848** Nexxtsolutions nebula300plus firmware

Nexxt Solutions Nebula 300+ firmware through version 12.01.01.37 uses the ecos_pw cookie for authentication, which contains Base64-encoded credential data combined with a static suffix. Because the encoding is reversible and lacks integrity protection, an atta

3 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

RuneScape Boards rsboards.com 222,762 accounts

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.