Daily brief, Friday, March 20, 2026

Mar 19, 8:00 PM to Mar 20, 8:00 PM ET

Generated Nov 7, 2026, 11:31 AM ET

0	5	0	39	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 newly exploited, 39 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

5

10.0 **CVE-2025-32432** Craft CMS Craft CMS CISA KEV DETECTION

A remote attacker can execute arbitrary code in Craft CMS through a code injection flaw; the input does not state whether authentication or user interaction is required.

9.2 **CVE-2025-54068** Laravel Livewire CISA KEV DETECTION

Unauthenticated attackers can achieve remote command execution in Laravel Livewire via code injection in specific scenarios.

8.8 **CVE-2025-31277** Apple Multiple Products CISA KEV

A buffer overflow in Apple Safari and iOS, macOS, iPadOS, watchOS, visionOS, and tvOS lets attackers corrupt memory via maliciously crafted web content.

7.8 **CVE-2025-43510** Apple Multiple Products CISA KEV

A malicious application on Apple watchOS, iOS, iPadOS, macOS, visionOS, and tvOS causes unexpected changes to memory shared between processes through improper locking.

5.5 **CVE-2025-43520** Apple Multiple Products CISA KEV

A classic buffer overflow in Apple watchOS, iOS, iPadOS, macOS, visionOS, and tvOS lets a malicious app crash the system or write kernel memory.

New public exploit code

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

New critical CVEs

39

10.0 **CVE-2025-32432** Craft CMS Craft CMS KEV EXPLOIT CODE DETECTION

A remote attacker can execute arbitrary code in Craft CMS through a code injection flaw; the input does not state whether authentication or user interaction is required.

9.2 **CVE-2025-54068** Laravel Livewire KEV EXPLOIT CODE DETECTION

Unauthenticated attackers can achieve remote command execution in Laravel Livewire via code injection in specific scenarios.

9.8 **CVE-2026-21992** Oracle Oracle Identity Manager

Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: REST WebServices) and Oracle Web Services Manager product of Oracle Fusion Middleware (component: Web Services Security). Supported versions that are affected are 12.2

9.8 **CVE-2026-3584** DETECTION

The Kali Forms plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.4.9 via the 'form_process' function. This is due to the 'prepare_post_data' function mapping user-supplied keys directly into internal placeholde

9.8 **CVE-2026-33057** Mesop-Dev mesop DETECTION

Mesop is a Python-based UI framework that allows users to build web applications. In versions 1.2.2 and below, an explicit web endpoint inside the ai/ testing module infrastructure directly ingests untrusted Python code strings unconditionally without authenti

9.8 **CVE-2025-15607** Tp-Link archer ax53 firmware

A command injection vulnerability on AX53 v1 occurs in mscd debug functionality due to insufficient input handling, allowing log redirection to arbitrary files and concatenation of unvalidated file content into shell commands, enabling authenticated attackers

9.1 **CVE-2026-33186** Grpc grpc

gRPC-Go is the Go language implementation of gRPC. Versions prior to 1.79.3 have an authorization bypass resulting from improper input validation of the HTTP/2 `:path` pseudo-header. The gRPC-Go server was too lenient in its routing logic, accepting requests w

9.8 **CVE-2026-32985** Apereo xerte online toolkits

Xerte Online Toolkits versions 3.14 and earlier contain an unauthenticated arbitrary file upload vulnerability in the template import functionality that allows remote attackers to execute arbitrary code by uploading a crafted ZIP archive containing malicious P

9.8 **CVE-2026-22901** Qnap qunetswitch

A command injection vulnerability has been reported to affect QuNetSwitch. If a remote attacker gains a user account, they can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following version: QuNet

9.1 **CVE-2026-33210** Ruby-Lang json

Ruby JSON is a JSON implementation for Ruby. From version 2.14.0 to before versions 2.15.2.1, 2.17.1.2, and 2.19.2, a format string injection vulnerability can lead to denial of service attacks or information disclosure, when the allow_duplicate_key: false par

9.8 **CVE-2026-33228** Webreflection flatted

flatted is a circular JSON parser. Prior to version 3.4.2, the parse() function in flatted can use attacker-controlled string values from the parsed JSON as direct array index keys, without validating that they are numeric. Since the internal input buffer is a

10.0 **CVE-2026-33054** Mesop-Dev mesop

Mesop is a Python-based UI framework that allows users to build web applications. Versions 1.2.2 and below contain a Path Traversal vulnerability that allows any user supplying an untrusted state_token through the UI stream payload to arbitrarily target files

9.8 **CVE-2026-22898** Qnap qvr pro

A missing authentication for critical function vulnerability has been reported to affect QVR Pro. The remote attackers can then exploit the vulnerability to gain access to the system. We have already fixed the vulnerability in the following version: QVR Pro 2.

9.8 **CVE-2026-32760** Filebrowser filebrowser

File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. In versions 2.61.2 and below, any unauthenticated visitor can register a full administrator account when self-registration

9.8 **CVE-2026-32771** Ctfer monitoring

The CTFer.io Monitoring component is in charge of the collection, process and storage of various signals (i.e. logs, metrics and distributed traces). In versions prior to 0.2.2, the sanitizeArchivePath function in pkg/extract/extract.go (lines 248–254) is vuln

9.8 **CVE-2025-15608** Tp-Link archer ax53 firmware

This vulnerability in AX53 v1, AX55 v4 and AX55 v4.6 results from insufficient input sanitization in the device's probe handling logic, where unvalidated parameters can trigger a stack-based buffer overflow that causes the affected service to crash and, under

9.0 **CVE-2026-33066** B3log siyuan

SiYuan is a personal knowledge management system. In versions 3.6.0 and below, the backend renderREADME function uses lute.New() without calling SetSanitize(true), allowing raw HTML embedded in Markdown to pass through unmodified. The frontend then assigns the

9.9 **CVE-2026-22172** Openclaw openclaw

OpenClaw versions prior to 2026.3.12 contain an authorization bypass vulnerability in the WebSocket connect path that allows shared-token or password-authenticated connections to self-declare elevated scopes without server-side binding. Attackers can exploit t

9.0 **CVE-2026-33067** B3log siyuan

SiYuan is a personal knowledge management system. Versions 3.6.0 and below render package metadata fields (displayName, description) using template literals without HTML escaping. A malicious package author can inject arbitrary HTML/JavaScript into these field

9.8 **CVE-2026-32767** B3log siyuan

SiYuan is a personal knowledge management system. Versions 3.6.0 and below contain an authorization bypass vulnerability in the /api/search/fullTextSearchBlock endpoint. When the method parameter is set to 2, the endpoint passes user-supplied input directly as

19 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.