Daily brief, Wednesday, April 1, 2026

Mar 31, 8:00 PM to Apr 1, 8:00 PM ET

Generated Nov 7, 2026, 9:47 AM ET

0	1	0	32	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 32 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.8 **CVE-2026-5281** Google Dawn CISA KEV

Google Dawn use-after-free lets a remote attacker with a compromised renderer run arbitrary code via a crafted HTML page, affecting Chromium-based products.

New public exploit code

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

New critical CVEs

32

9.8 **CVE-2026-20160** Cisco smart software manager on-prem

A vulnerability in Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected SSM On-Prem host. This vulnerability is due to the unintention

9.6 **CVE-2026-5289** Google chrome

Use after free in Navigation in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-5288** Google chrome

Use after free in WebView in Google Chrome on Android prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-5290** Google chrome

Use after free in Compositing in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.1 **CVE-2026-33990** Docker model runner

Docker Model Runner (DMR) is software used to manage, run, and deploy AI models using Docker. Prior to version 1.1.25, Docker Model Runner contains an SSRF vulnerability in its OCI registry token exchange flow. When pulling a model, Model Runner follows the re

9.8 **CVE-2026-29014** Metinfo metinfo DETECTION

MetInfo CMS versions 7.9, 8.0, and 8.1 contain an unauthenticated PHP code injection vulnerability that allows remote attackers to execute arbitrary code by sending crafted requests with malicious PHP code. Attackers can exploit insufficient input neutralizati

9.8 **CVE-2026-34159** Ggml llama.cpp

llama.cpp is an inference of several LLM models in C/C++. Prior to version b8492, the RPC backend's deserialize_tensor() skips all bounds validation when a tensor's buffer field is 0. An unauthenticated attacker can read and write arbitrary process memory via

9.8 **CVE-2024-43028** Jeecg jeecg boot

A command injection vulnerability in the component /jmreport/show of jeecg boot v3.0.0 to v3.5.3 allows attackers to execute arbitrary code via a crafted HTTP request.

9.8 **CVE-2026-20093**

A vulnerability in the change password functionality of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to bypass authentication and gain access to the system as Admin. This vulnerability is due to incorrect ha

9.8 **CVE-2026-31027** Totolink a3600r firmware

TOTOlink A3600R v5.9c.4959 contains a buffer overflow vulnerability in the setAppEasyWizardConfig interface of /lib/cste_modules/app.so. The vulnerability occurs because the rootSsid parameter is not properly validated for length, allowing remote attackers to

9.8 **CVE-2026-30643** Dedecms dedecms

An issue was discovered in DedeCMS 5.7.118 allowing attackers to execute code via crafted setup tag values in a module upload.

9.8 **CVE-2024-40489** Jeecg jeecg boot

There is an injection vulnerability in jeecg boot versions 3.0.0 to 3.5.3 due to lax character filtering, which allows attackers to execute arbitrary code on components through specially crafted HTTP requests.

9.1 **CVE-2026-34520** Aiohttp aiohttp

AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.13.4, the C parser (the default for most installs) accepted null bytes and control characters in response headers. This issue has been patched in version 3.13.4.

9.1 **CVE-2026-34456** Reviactyl reviactyl

Reviactyl is an open-source game server management panel built using Laravel, React, FilamentPHP, Vite, and Go. From version 26.2.0-beta.1 to before version 26.2.0-beta.5, a vulnerability in the OAuth authentication flow allowed automatic linking of social acc

9.8 **CVE-2025-71279** Xenforo xenforo

XenForo before 2.3.7 contains a security issue affecting Passkeys that have been added to user accounts. An attacker may be able to compromise the security of Passkey-based authentication.

9.9 **CVE-2026-34571** Ci4-Cms-Erp ci4ms

+9 more CVEs in the same release

CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.31.0.0, a Stored Cross-Site Scripting (Stored XSS) vulnerability exists in the backend user managem

10.0 **CVE-2026-4370** Canonical juju

A vulnerability was identified in Juju from version 3.2.0 until 3.6.19 and from version 4.0 until 4.0.4, where the internal Dqlite database cluster fails to perform proper TLS client and server authentication. Specifically, the Juju controller's database endpo

9.8 **CVE-2026-34875** Trustedfirmware mbed tls

An issue was discovered in Mbed TLS through 3.6.5 and TF-PSA-Crypto 1.0.0. A buffer overflow can occur in public key export for FFDH keys.

9.1 **CVE-2026-34751** Payloadcms payload

Payload is a free and open source headless content management system. Prior to version 3.79.1 in @payloadcms/graphql and payload, a vulnerability in the password recovery flow could allow an unauthenticated attacker to perform actions on behalf of a user who i

9.1 **CVE-2026-34873** Trustedfirmware mbed tls

An issue was discovered in Mbed TLS 3.5.0 through 4.0.0. Client impersonation can occur while resuming a TLS 1.3 session.

3 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

SUCCESS success.com 253,510 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.