Daily brief, Tuesday, March 24, 2026

Mar 23, 8:00 PM to Mar 24, 8:00 PM ET

Generated Nov 7, 2026, 10:59 AM ET

0	0	0	48	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

48 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

48

9.8 **CVE-2026-4696** Mozilla firefox

Use-after-free in the Layout: Text and Fonts component. This vulnerability was fixed in Firefox 149, Firefox ESR 115.34, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4700** Mozilla firefox

Mitigation bypass in the Networking: HTTP component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4698** Mozilla firefox

JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 149, Firefox ESR 115.34, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4702** Mozilla firefox

JIT miscompilation in the JavaScript Engine component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

10.0 **CVE-2026-4689** Mozilla firefox

Sandbox escape due to incorrect boundary conditions, integer overflow in the XPCOM component. This vulnerability was fixed in Firefox 149, Firefox ESR 115.34, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4705** Mozilla firefox

Undefined behavior in the WebRTC: Signaling component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4723** Mozilla firefox

Use-after-free in the JavaScript Engine component. This vulnerability was fixed in Firefox 149 and Thunderbird 149.

9.6 **CVE-2026-33211** Linuxfoundation tekton pipelines

Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. Starting in version 1.0.0 and prior to versions 1.0.1, 1.3.3, 1.6.1, 1.9.2, and 1.10.2, the Tekton Pipelines git resolver is vulnerable to path traversal via the `pathIn

10.0 **CVE-2026-4688** Mozilla firefox

Sandbox escape due to use-after-free in the Disability Access APIs component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.1 **CVE-2026-4724** Mozilla firefox

Undefined behavior in the Audio/Video component. This vulnerability was fixed in Firefox 149 and Thunderbird 149.

10.0 **CVE-2026-4692** Mozilla firefox

Sandbox escape in the Responsive Design Mode component. This vulnerability was fixed in Firefox 149, Firefox ESR 115.34, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4691** Mozilla firefox

Use-after-free in the CSS Parsing and Computation component. This vulnerability was fixed in Firefox 149, Firefox ESR 115.34, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4701** Mozilla firefox

Use-after-free in the JavaScript Engine component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.1 **CVE-2026-4715** Mozilla firefox

Uninitialized memory in the Graphics: Canvas2D component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4720** Mozilla firefox

Memory safety bugs present in Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary cod

9.8 **CVE-2026-4721** Mozilla firefox

Memory safety bugs present in Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited

9.8 **CVE-2026-4717** Mozilla firefox

Privilege escalation in the Netmonitor component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4710** Mozilla firefox

Incorrect boundary conditions in the Audio/Video component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.1 **CVE-2026-4716** Mozilla firefox

Incorrect boundary conditions, uninitialized memory in the JavaScript Engine component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

9.8 **CVE-2026-4711** Mozilla firefox

Use-after-free in the Widget: Cocoa component. This vulnerability was fixed in Firefox 149, Firefox ESR 140.9, Thunderbird 149, and Thunderbird 140.9.

28 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.