Daily brief, Tuesday, February 24, 2026

Feb 23, 7:00 PM to Feb 24, 7:00 PM ET

Generated Nov 7, 2026, 4:02 PM ET

0	1	0	68	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 68 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.8 **CVE-2026-25108** Soliton Systems K.K FileZen CISA KEV

Soliton Systems FileZen OS command injection lets an authenticated user execute OS commands on the server via a crafted HTTP request.

New public exploit code

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

New critical CVEs

68

9.8 **CVE-2026-2796** Mozilla firefox

JIT miscompilation in the JavaScript: WebAssembly component. This vulnerability was fixed in Firefox 148 and Thunderbird 148.

9.8 **CVE-2026-2773** Mozilla firefox

Incorrect boundary conditions in the Web Audio component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2774** Mozilla firefox

Integer overflow in the Audio/Video component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2775** Mozilla firefox

Mitigation bypass in the DOM: HTML Parser component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2771** Mozilla firefox

Undefined behavior in the DOM: Core & HTML component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2763** Mozilla firefox

Use-after-free in the JavaScript Engine component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2764** Mozilla firefox

JIT miscompilation, use-after-free in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2765** Mozilla firefox

+1 more CVEs in the same release

Use-after-free in the JavaScript Engine component. This vulnerability was fixed in Firefox 148, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2766** Mozilla firefox

Use-after-free in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 148, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2770** Mozilla firefox

Use-after-free in the DOM: Bindings (WebIDL) component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2772** Mozilla firefox

Use-after-free in the Audio/Video: Playback component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2779** Mozilla firefox

Incorrect boundary conditions in the Networking: JAR component. This vulnerability was fixed in Firefox 148, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2788** Mozilla firefox

Incorrect boundary conditions in the Audio/Video: GMP component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2805** Mozilla firefox

Invalid pointer in the DOM: Core & HTML component. This vulnerability was fixed in Firefox 148 and Thunderbird 148.

9.8 **CVE-2026-2787** Mozilla firefox

Use-after-free in the DOM: Window and Location component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2762** Mozilla firefox

Integer overflow in the JavaScript: Standard Library component. This vulnerability was fixed in Firefox 148, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2791** Mozilla firefox

Mitigation bypass in the Networking: Cache component. This vulnerability was fixed in Firefox 148, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2757** Mozilla firefox

Incorrect boundary conditions in the WebRTC: Audio/Video component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2785** Mozilla firefox

Invalid pointer in the JavaScript Engine component. This vulnerability was fixed in Firefox 148, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

9.8 **CVE-2026-2758** Mozilla firefox

Use-after-free in the JavaScript: GC component. This vulnerability was fixed in Firefox 148, Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird 148, and Thunderbird 140.8.

47 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.