Daily brief, Tuesday, June 16, 2026

Jun 15, 8:00 PM to Jun 16, 8:00 PM ET

Generated Nov 4, 2026, 9:23 PM ET

0	1	0	19	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 19 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2026-48907** Widget Factory Joomla Content Editor CISA KEV DETECTION

An attacker can upload and execute PHP code on a Widget Factory Joomla Content Editor server.

New public exploit code

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

New critical CVEs

19

10.0 **CVE-2026-48907** Widget Factory Joomla Content Editor KEV EXPLOIT CODE DETECTION

An attacker can upload and execute PHP code on a Widget Factory Joomla Content Editor server.

9.8 **CVE-2026-12293** Mozilla firefox

Use-after-free in the Graphics: WebGPU component. This vulnerability was fixed in Firefox 152 and Thunderbird 152.

9.8 **CVE-2026-0126** Google android

In WC-Radio, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

9.6 **CVE-2026-12294** Mozilla firefox

Sandbox escape in the DOM: Workers component. This vulnerability was fixed in Firefox 152, Firefox ESR 140.12, Firefox ESR 115.37, Thunderbird 152, and Thunderbird 140.12.

9.6 **CVE-2026-12295** Mozilla firefox
Sandbox escape in the DOM: Navigation component. This vulnerability was fixed in Firefox 152, Firefox ESR 140.12, Firefox ESR 115.37, Thunderbird 152, and Thunderbird 140.12.

9.6 **CVE-2026-12296** Mozilla firefox
Sandbox escape in the Security: Process Sandboxing component. This vulnerability was fixed in Firefox 152, Firefox ESR 140.12, Thunderbird 152, and Thunderbird 140.12.

9.6 **CVE-2026-12297** Mozilla firefox
Sandbox escape due to incorrect boundary conditions in the Networking component. This vulnerability was fixed in Firefox 152, Firefox ESR 140.12, Firefox ESR 115.37, Thunderbird 152, and Thunderbird 140.12.

9.1 **CVE-2026-12304** Mozilla firefox
Same-origin policy bypass in the Networking: Cookies component. This vulnerability was fixed in Firefox 152, Firefox ESR 140.12, Thunderbird 152, and Thunderbird 140.12.

9.1 **CVE-2026-12315** Mozilla firefox
Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 152, Firefox ESR 140.12, Thunderbird 152, and Thunderbird 140.12.

9.1 **CVE-2026-12316** Mozilla firefox
Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 152 and Thunderbird 152.

9.9 **CVE-2026-49774**
Improper Control of Generation of Code ('Code Injection') vulnerability in Filipe Nasc RD Station allows Remote Code Inclusion. This issue affects RD Station: from n/a through 5.6.0.

9.9 **CVE-2026-40750**
Unrestricted Upload of File with Dangerous Type vulnerability in themagnifico52 Kids Online Store allows Upload a Web Shell to a Web Server. This issue affects Kids Online Store: from n/a through 0.8.9.

9.3 **CVE-2026-39574**
Unauthenticated SQL Injection in InPost Gallery <= 2.1.4.6 versions.

9.3 **CVE-2026-49772** DETECTION
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Liquid Web / StellarWP The Events Calendar allows Blind SQL Injection. This issue affects The Events Calendar: from 6.15.12 through 6.16.2.

9.3 **CVE-2026-52715** DETECTION
Unauthenticated SQL Injection in GEO my WordPress <= 4.5.5 versions.

9.3 **CVE-2026-48777**
FileBrowser Quantum is a free, self-hosted, web-based file manager. Versions prior to 1.3.2-stable, 1.4.0-beta and 1.4.1-beta are vulnerable to Path Traversal through the publicPatchHandler in backend/http/public.go which joins user-controlled fromPath and toP

9.2 **CVE-2025-13036**

An authentication bypass security issue exists within FactoryTalk Historian Site Edition. By continually sending requests to the login endpoint, an attacker may obtain a valid authentication token.

9.1 **CVE-2026-53776**

Perry before 0.5.1166 contains a JWT validation vulnerability that allows remote attackers to bypass token expiration by exploiting the unconditional setting of validate_exp = false in the verify_decode helper within the stdlib JWT verification path. Attackers

9.1 **CVE-2026-22313**

The device has a webserver that exposes a REST API authenticated with a token on the management network. By exploiting an OS command injection vulnerability an authenticated attacker can send arbitrary commands to the device that are executed with administrati

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. CVE IDs link to the full record on Watch Floor.