Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Firefox Users at Risk: Two Major Flaws Found and Fixed

Date of Publication	Admiralty Code	TA Number
May 20, 2025	A1	TA2025156

Summary

First Seen: May 17, 2025
Affected Products: Mozilla Firefox, Firefox ESR
Impact: Mozilla has rushed out emergency updates to fix two critical bugs in Firefox that hackers exploited even before they were publicly known. These flaws, revealed during the Pwn2Own hacking contest, could let attackers mess with browser memory and potentially run malicious code or steal sensitive data. The issues tracked as CVE-2025-4918 and CVE-2025-4919 involve how Firefox handles JavaScript promises and array math. If you're using Firefox and haven't updated yet, you're at risk. Make sure to upgrade to the latest version to stay protected.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-4918	Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	Mozilla Firefox Firefox ESR	✓	✗	✓
CVE-2025-4919	Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	Mozilla Firefox Firefox ESR	✓	✗	✓

Vulnerability Details

#1 Mozilla has urgently released patches for two critical zero-day vulnerabilities affecting its Firefox browser. These security flaws were discovered after being actively exploited during the Pwn2Own Berlin hacking competition, highlighting their real-world impact. Tracked as CVE-2025-4918 and CVE-2025-4919, both vulnerabilities could allow attackers to gain unauthorized access to sensitive information or execute malicious code on a user's system.

#2 CVE-2025-4918 stems from how Firefox handles JavaScript Promises. The bug leads to an out-of-bounds access issue, meaning an attacker could read or write data outside the normal memory boundaries of a JavaScript object. Similarly, CVE-2025-4919 involves a flaw in how Firefox optimizes specific mathematical operations, which can be exploited to manipulate memory handling. It allows attackers to confuse the way array index sizes are handled, again leading to unauthorized memory access.

#3 If exploited, these vulnerabilities could allow threat actors to carry out actions like stealing private data, bypassing security protections, or crashing and taking control of the browser. In some cases, this might even be used as a steppingstone to launch broader attacks on the system. The risks include full remote code execution essentially letting an attacker run arbitrary code on the victim's machine.

#4 To stay safe, Mozilla strongly recommends that users update their browsers immediately. The fixes are available in Firefox version 138.0.4, and in the extended support releases ESR 128.10.1 and ESR 115.23.1. Promptly applying these updates is essential to close off the vulnerabilities before they can be further abused in the wild.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-4918	Mozilla Firefox Version Prior to 138.0.4 Firefox ESR Version Prior to 128.10.1 Firefox ESR Version Prior to 115.23.1	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*:*	CWE-125
CVE-2025-4919	Mozilla Firefox Version Prior to 138.0.4 Firefox ESR Version Prior to 128.10.1 Firefox ESR Version Prior to 115.23.1	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*:*	CWE-787 CWE-125

Recommendations

Update Firefox: Mozilla has released fixed versions to patch these security holes. If you're using Firefox, go ahead and update it to the latest version-138.0.4. If you're using the Extended Support Release (ESR), make sure you're on 128.10.1 or 115.23.1.

Turn On Auto-Updates: To make life easier, turn on automatic updates in your Firefox settings. That way, you'll always have the latest security fixes without needing to remember to check manually.

Be Careful on Suspicious Websites: While Mozilla has patched the issue, it's always a good idea to avoid shady websites. You can also install tools to block potentially harmful scripts from running in your browser.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1059.007** JavaScript	**T1190** Exploit Public-Facing Application
T1203 Exploitation for Client Execution			

Patch Details

Update your Mozilla Firefox to the latest version to address the flaws.
For Firefox Upgrade to Version 138.0.4
For Firefox ESR Upgrade to Version 128.10.1 or 115.23.1

Link:
https://www.mozilla.org/en-US/firefox/138.0.4/releasenotes/

https://www.mozilla.org/en-US/firefox/128.10.1/releasenotes/

https://www.mozilla.org/en-US/firefox/115.23.1/releasenotes/

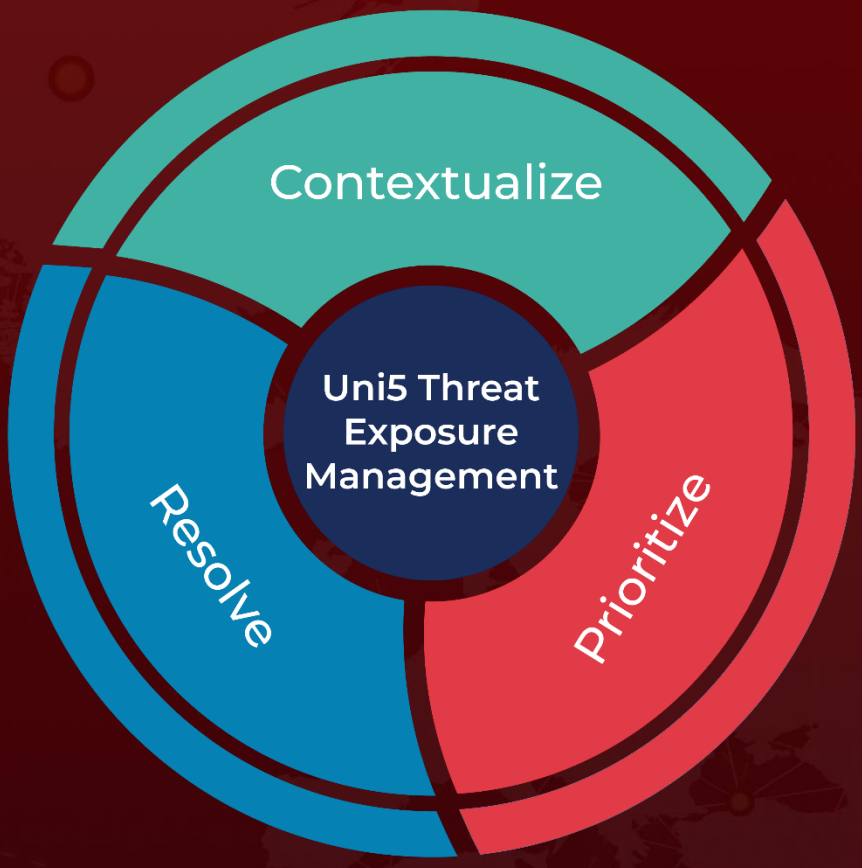
References

https://www.mozilla.org/en-US/security/advisories/mfsa2025-36/#CVE-2025-4918

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 20, 2025 • 4:45 AM

More at www.hivepro.com