Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Firefox Zero-Day Alert: Critical Animation Timeline Flaw Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
October 10, 2024	A1	TA2024388

Summary

First Seen: October 9, 2024
Affected Products: Mozilla Firefox and Firefox ESR
Impact: Mozilla has released a security update for Firefox to patch a critical zero-day use-after-free vulnerability, designated as CVE-2024-9680. This flaw, found within Animation Timelines, is actively being exploited in the wild, posing a significant threat to users. If left unpatched, this vulnerability could allow attackers to execute arbitrary code, potentially compromising systems. It is imperative that users update their Firefox browsers promptly to safeguard against this ongoing exploitation and prevent further security breaches.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-9680	Mozilla Firefox Use-After-Free Vulnerability	Mozilla Firefox and Firefox ESR	✓	✓	✓

Vulnerability Details

#1

The Mozilla Foundation has revealed a zero-day vulnerability in its popular web browser, Firefox, designated as CVE-2024-9680. This critical flaw is identified as use-after-free issue within Firefox’s animation timelines, which displays a synchronized graphic representation for all animations applied to a specific element or its children. This vulnerability allows attackers to execute arbitrary code potentially leading to system compromise.

#2

The vulnerability results from improper memory access, where previously freed memory is still utilized, granting threat actors the potential to seize control of affected systems. The Mozilla Foundation has confirmed that CVE-2024-9680 is being actively exploited in the wild, heightening its severity. Given the critical nature of this vulnerability, users are urged to update their Firefox browser immediately to mitigate any risk of exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-9680	Firefox Version Prior to 131.0.2, Firefox ESR Version Prior to 128.3.1, and Firefox ESR Version Prior to 115.16.1	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*	CWE-416

Recommendations

Update: Users are strongly encouraged to upgrade to the latest versions, which contain critical fixes for the identified vulnerability. To upgrade to the latest version, simply launch Firefox and navigate to Settings → Help → About Firefox. The update process will initiate automatically, ensuring that your browser remains secure against potential threats.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Regular Audits and Monitoring for Browser Security: To strengthen the browser security, it is essential to implement regular audits focused on identifying signs of exploitation and abnormal activity in web applications and browser configurations. Conduct these audits periodically, with additional ad-hoc assessments triggered by critical updates, configuration changes, or suspected security incidents.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1588.005** Exploits	**T1189** Drive-by Compromise	**T1059** Command and Scripting Interpreter

Patch Details

Users operating on outdated versions of Firefox, or the Extended Support Release (ESR) are strongly urged to upgrade to the latest releases without delay to mitigate the risk. The recommended updates are as follows:
Firefox: 131.0.2
Firefox ESR: 115.16.1
Firefox ESR: 128.3.1

Links: https://www.mozilla.org/en-US/firefox/download/thanks/

https://www.mozilla.org/en-US/firefox/enterprise/#download

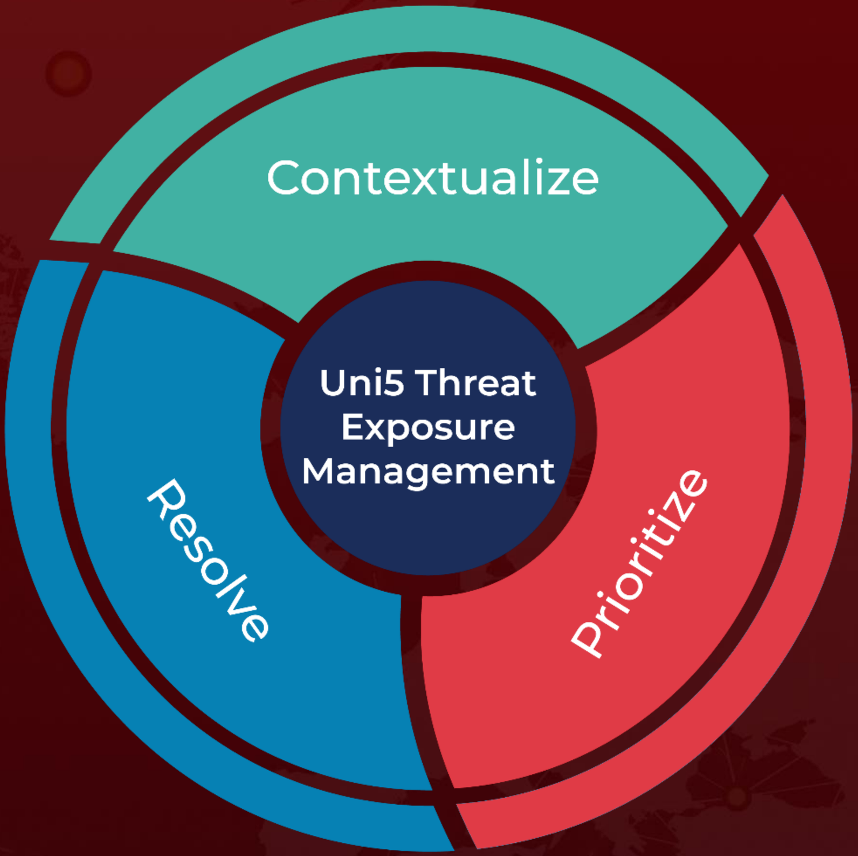
References

https://www.mozilla.org/en-US/security/advisories/mfsa2024-51/

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

October 10, 2024 • 8:45 AM

More at www.hivepro.com