CVE-2025-49710

15/06/2025

Critical Firefox Vulnerability: Integer Overflow in JavaScript Engine (CVSS 9.8)

CONFIDENTIAL

Executive Summary

CVE-2025-49710 is a critical vulnerability in Mozilla Firefox affecting versions prior to 139.0.4, rated CVSS 9.8. The flaw resides in the JavaScript engine's OrderedHashTable structure and allows remote attackers to exploit an integer overflow, potentially leading to arbitrary code execution. Mozilla patched the issue on June 10, 2025, and all users and organizations are strongly urged to update immediately.

Analysis

The vulnerability stems from an integer overflow during hash table size calculations in Firefox's JavaScript engine (OrderedHashTable). If an attacker crafts malicious JavaScript to exploit this flaw, it can cause memory corruption due to misallocated memory regions. This could enable remote code execution without user interaction. The issue is especially dangerous because it can be triggered via websites, making it suitable for drive-by attacks or exploitation chains in the wild. The patch in version 139.0.4 adjusts internal bounds checking to prevent overflow conditions.

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-49710

Versions affected

- **All versions prior to 139.0.4**

Solutions

To mitigate the vulnerability, update Firefox to version 139.0.4 or later, which contains the official patch addressing the vulnerability. This update fixes an integer overflow issue in the JavaScript engine that could allow remote code execution. Users can update through Firefox's built-in updater or download the latest version directly from Mozilla's website. Until the update is applied, it’s recommended to avoid untrusted websites and disable JavaScript where possible.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.