CVE-2025-2857: Firefox Sandbox Escape

Vairav CVE Report

Date: March 28, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A critical vulnerability, identified as CVE-2025-2857, has been discovered in Mozilla Firefox for Windows. This flaw allows attackers to escape the browser's sandbox environment, potentially leading to arbitrary code execution on affected systems. The CVSS score has yet to be assigned.

VULNERABILITY DETAILS

CVE-2025-2857

- **Description:** The vulnerability arises from improper handling within Firefox's inter-process communication (IPC) code. A compromised child process can manipulate the parent process into leaking handles, granting unprivileged child processes unintended elevated access. This mismanagement facilitates a sandbox escape, allowing attackers to execute code outside the browser's secure environment.
- **Impact:** Exploitation of this vulnerability enables attackers to break out of Firefox's sandbox on Windows systems, potentially leading to full system compromise. While there is no current evidence of active exploitation, the similarity to a recently exploited Chrome zero-day (CVE-2025-2783) underscores the potential risk.
- **CVSS Score:** N/A

AFFECTED VERSIONS

The following Firefox versions for Windows are affected:

- Firefox versions prior to 136.0.4
- Firefox Extended Support Release (ESR) versions prior to 128.8.1
- Firefox ESR versions prior to 115.21.1

EXPLOIT DETAILS

This vulnerability particularly impacts environments where Firefox is utilized on Windows systems. Attackers can exploit the flaw by crafting malicious child processes that manipulate the parent process into leaking handles. This manipulation leads to a sandbox escape, allowing the execution of arbitrary code outside the browser's secure environment.

While there is no current evidence of active exploitation, the similarity to the recently patched Chrome zero-day (CVE-2025-2783) highlights the potential risk.

RECOMMENDED ACTIONS

Patch & Upgrade:

Users and administrators are strongly advised to upgrade to the latest Firefox versions to mitigate this vulnerability:

- **Firefox:**
  - Upgrade to version 136.0.4 or later.
- **Firefox ESR:**
  - Upgrade to version 115.21.1 or later.
  - Upgrade to version 128.8.1 or later.

ADDITIONAL SECURITY MEASURES

- **Regular Software Updates**: Ensure all software, especially web browsers, are kept up to date with the latest security patches.
- **Security Audits**: Conduct regular security audits of systems to identify and address potential vulnerabilities.
- **User Awareness Training**: Educate users about the risks of phishing and unsafe browsing practices that could lead to exploitation.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-2857
- https://thehackernews.com/2025/03/mozilla-patches-critical-firefox-bug.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com