NATIONAL
CSIRT CY

CVE-2025-2857

Firefox sandbox escape flaw

30/3/2025

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

A compromised child process could cause the parent process to return an unintentionally powerful handle, leading to a sandbox escape.

Following the recent Chrome sandbox escape (CVE-2025-2783), various Firefox developers identified a similar pattern in the IPC code.

**This only affects Firefox on Windows. Other operating systems are unaffected.

Analysis

This vulnerability affects Firefox < 136.0.4, Firefox ESR < 128.8.1, and Firefox ESR < 115.21.1.

https://www.mozilla.org/en-US/security/advisories/mfsa2025-19/#CVE-2025-2857

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-2857

Solutions

Fixed in:

- Firefox 136.0.4
- Firefox ESR 115.21.1
- Firefox ESR 128.8.1

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.