

HiveForce Labs

# THREAT ADVISORY



## VULNERABILITY REPORT

### **Critical Firefox Flaw CVE-2025-2857 Lets Attackers Escape Sandbox**

Date of Publication

May 8, 2025

Admiralty Code

A1

TA Number

TA2025140




# Summary

**First Seen:** March 2025

**Affected Product:** Mozilla Firefox

**Impact:** CVE-2025-2857 is a critical vulnerability in Mozilla Firefox for Windows, with a maximum CVSS score of 10.0. It allows a compromised child process to exploit the IPC system and escape the browser's sandbox, potentially leading to remote code execution. The flaw affects Firefox versions before 136.0.4 and ESR versions before 128.8.1 and 115.21.1, with no impact on other operating systems. Although similar to a Chrome bug that was exploited in the wild, there is no evidence that this Firefox vulnerability has been actively used in attacks.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-2857	Mozilla Firefox Sandbox Escape Vulnerability	Mozilla Firefox			

# Vulnerability Details

## #1

CVE-2025-2857 is a critical vulnerability affecting Mozilla Firefox on Windows systems, publicly disclosed on March 27, 2025. It carries a CVSS v3.1 base score of 10.0, indicating its maximum severity under current scoring standards. This flaw poses a significant risk, allowing potential attackers to break out of Firefox's security sandbox and execute code with the privileges of the user.

## #2

The vulnerability originates in Firefox's inter-process communication (IPC) mechanism. A malicious child process (such as one running web content) could exploit the flaw to trick the parent browser process into returning a handle with elevated permissions. This flaw allows a sandbox escape, undermining one of the core protections in Firefox's security model. It was discovered following the disclosure of a similar Chrome vulnerability ([CVE-2025-2783](#)), which was exploited in targeted attacks. However, CVE-2025-2857 itself has not been exploited in the wild as of the latest available information.

# #3

Only Windows versions of Firefox are affected. The vulnerability impacts Firefox versions prior to 136.0.4, and Firefox ESR versions prior to 128.8.1 and 115.21.1. Systems running Firefox on Linux, macOS, or other operating systems are not affected by this flaw.

# #4

Successful exploitation requires no user interaction or authentication, and could lead to remote code execution on the system. This makes the vulnerability particularly dangerous for enterprise and government environments. Users are strongly urged to update Firefox to version 136.0.4 or the appropriate ESR version immediately to mitigate this critical risk.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-2857	Firefox versions prior to 136.0.4 Firefox ESR versions prior to 128.8.1 Firefox ESR versions prior to 115.21.1	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*	CWE-20

## Recommendations



**Update Firefox Immediately:** Upgrade to Firefox 136.0.4 or later on Windows systems. For ESR users, update to Firefox ESR 128.8.1 or 115.21.1 depending on your release track. If you use Tor Browser on Windows, update to version 14.0.8 which includes the fix for this flaw.



**Restrict Use of Outdated Versions:** Proactively block or uninstall older versions of Firefox on Windows systems using configuration management tools or endpoint security controls.



**Monitor for Unusual Process Activity:** Use endpoint detection and response (EDR) tools to watch for suspicious inter-process communication or unexpected child process behavior from Firefox.



**Enforce Least Privilege:** Limit user privileges on Windows workstations to reduce the impact of potential sandbox escapes.

**Consider Browser Privacy Settings:** Enhance Firefox privacy by enabling Enhanced Tracking Protection, disabling data collection, and using privacy-focused search engines to reduce attack surface



## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0002</u></b> Execution	<b><u>TA0004</u></b> Privilege Escalation
<b><u>T1497</u></b> Virtualization/Sandbox Evasion	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.005</u></b> Exploits	<b><u>T1588.006</u></b> Vulnerabilities
<b><u>T1611</u></b> Escape to Host	<b><u>T1059</u></b> Command and Scripting Interpreter		



## Patch Details

Mozilla has addressed this vulnerability in the following versions:

- Firefox 136.0.4
- Firefox ESR 128.8.1
- Firefox ESR 115.21.1

Link:

<https://www.mozilla.org/en-US/security/advisories/mfsa2025-19/>



## References

<https://threatprotect.qualys.com/2025/03/28/mozilla-firefox-addresses-sandbox-escape-vulnerability-cve-2025-2857/>

<https://www.helpnetsecurity.com/2025/03/28/critical-firefox-tor-browser-sandbox-escape-flaw-fixed-cve-2025-2857/>

<https://securityaffairs.com/175945/security/mozilla-fixed-critical-firefox-vulnerability-cve-2025-2857.html>

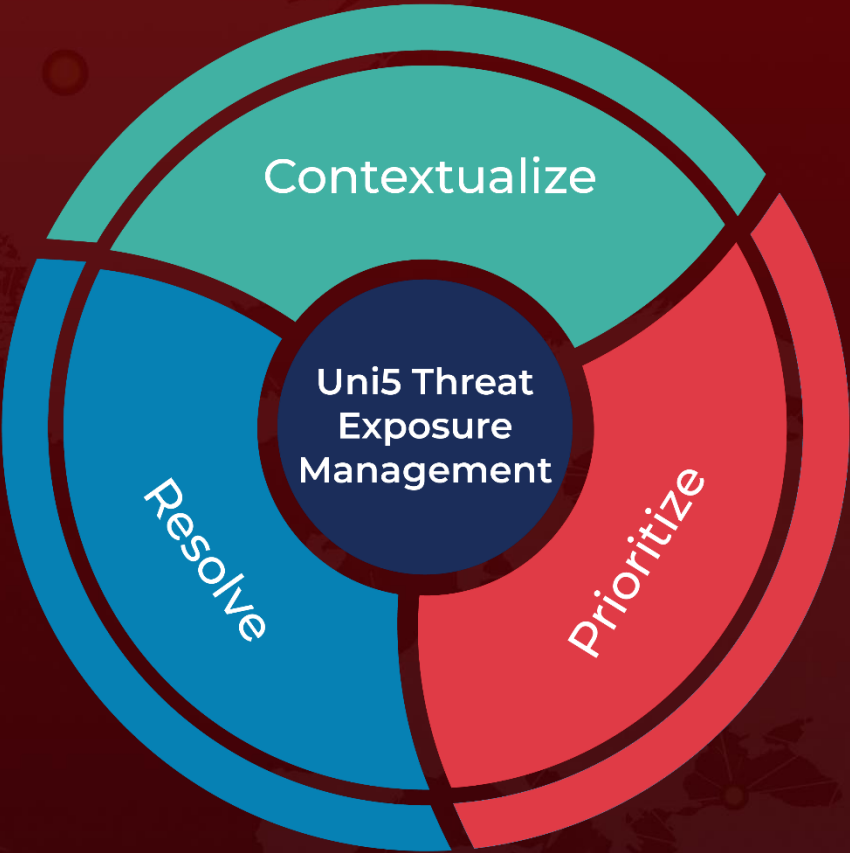
<https://hivepro.com/threat-advisory/chrome-zero-day-exploited-in-operation-forumtroll/>



# 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 8, 2025 • 7:30 AM**

