CVE-2025-25000: Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability

Vairav CVE Report

Date: April 4, 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 severe remote code execution (RCE) vulnerability, identified as **CVE-2025-25000**, has been reported in Microsoft Edge. This flaw arises from a type confusion error within the browser's underlying code and has been assigned **CVSS score of 8.8 (High)**. If exploited, it could allow attackers to execute arbitrary code on a user's system, potentially leading to full system compromise.

VULNERABILITY DETAILS

CVE-2025-25000

- **Description:** This vulnerability stems from a type confusion error in Microsoft Edge's Chromium-based architecture. Specifically, the browser may misinterpret data types when processing web content, leading to unpredictable behavior. An attacker can exploit this flaw by crafting a malicious webpage that, when visited, triggers the type confusion, resulting in the execution of arbitrary code with the privileges of the current user.
- **Impact:** Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code on the affected system. If the user has administrative privileges, the attacker could gain complete control over the system, leading to potential data theft, malware installation, and further network compromise.
- **CVSS Score:** 8.8 (High)

AFFECTED VERSIONS

All versions of Microsoft Edge (Chromium-based) prior to build 135.0.3179.54 are affected by this vulnerability.

EXPLOIT DETAILS

In a real-world attack scenario, an attacker could host a malicious webpage designed to exploit this type confusion vulnerability. By enticing users to visit this webpage—through phishing emails, malicious advertisements, or compromised legitimate sites—the attacker can trigger the vulnerability. Upon visiting the page, the malicious code would execute with

the same privileges as the user running the browser. Users with administrative rights are at heightened risk, as the attacker could gain full system control.

RECOMMENDED ACTIONS

Patch & Upgrade:

Upgrade Microsoft Edge (Chromium-based) to version 135.0.3179.54 or later to mitigate this vulnerability.

ADDITIONAL SECURITY MEASURES

- **Limit Administrative Privileges**: Operate browsers and other applications using accounts with the least privileges necessary. This practice minimizes the potential impact of vulnerabilities that may be exploited.
- **Enable Automatic Updates**: Configure Microsoft Edge to update automatically, ensuring that security patches are applied promptly without user intervention.
- **Educate Users**: Train users to recognize and avoid phishing attempts and suspicious links, reducing the likelihood of visiting malicious websites designed to exploit browser vulnerabilities.

REFERENCES

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-25000

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