Severity: High

Date: 30th August 2023

Summary

Microsoft Edge has published a release note that mentioned a Privilege escalation vulnerability with the CVE ID of CVE-2023-36741 and has a CVSS Score of 8.3 (High). This vulnerability exists in the Microsoft-Edge Chromium-based versions prior to 116.0.1938.62.

An unauthorized remote attacker can exploit this vulnerability which requires the interaction of the user. The scope of this vulnerability is beyond the vulnerable component of Microsoft Edge. There is no known exploit code available for this vulnerability.

Technical Details

Microsoft has not provided any additional details about this vulnerability which limits the current knowledge about this vulnerability.

However, Microsoft mentioned in their security advisory that this vulnerability affects the CIA (Confidentiality, Integrity, and Availability) of the affected application and its environment.

In addition, Tenable has released new plugins for Nessus, which users can use to detect this vulnerability. The plugin is as follows.

ID	Name	Product	Family	Severity
180197	Microsoft Edge (Chromium) < 116.0.1938.62 Multiple Vulnerabilities	Nessus	Windows	HIGH

During the previous release notes on August 21, 2023, Microsoft patched two vulnerabilities CVE-2023-38158 & CVE-2023-36787. These vulnerabilities were information disclosure and elevation of privileges patched in the versions Microsoft Edge Stable and Extended Stable Channel (Version 116.0.1938.54).

However, in this current release note, Microsoft has patched only one Elevation of privileges vulnerability, which is the 4th patch update this month. As of the month of July, only two release notes were released.

Action Plan

Users of Chromium-based Microsoft Edge are recommended to upgrade to the latest version in order to fix this vulnerability and prevent exploitation.

Reference Links

https://gbhackers.com/microsoft-edge-privilege-escalation-flaw/