Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability

Severity Level: High

Components Affected

- Microsoft Edge (Chromium-based) versions prior to **150.0.4078.48**

Overview

A remote code execution (RCE) vulnerability has been identified in Microsoft Edge (Chromium-based) due to improper handling of untrusted data during the deserialization process. If successfully exploited, vulnerability could allow an attacker to execute arbitrary code on a victim's system. Exploitation requires convincing a user to visit a specially crafted malicious website or open attacker-controlled content. Depending on the privileges of the affected user, an attacker may be able to install programs, modify or delete data, create new user accounts, or perform other unauthorized actions on the compromised system.

Description

Microsoft has released security updates to address a remote code execution vulnerability in Microsoft Edge (Chromium-based), tracked as CVE-2026-58281. The vulnerability is caused by improper deserialization of untrusted data, where Microsoft Edge incorrectly processes specially crafted input.

An attacker could exploit this vulnerability by hosting a malicious website or distributing specially crafted content through phishing emails, instant messages, or other communication channels. To successfully exploit the vulnerability, the attacker must persuade a user to visit the malicious webpage or open the attacker-controlled content and perform the required interactions that trigger the flaw.

Successful exploitation could allow arbitrary code to execute in the security context of the logged-in user. Systems where users have administrative privileges are at greater risk, as an attacker may gain the ability to install malicious software, manipulate or delete sensitive information, create new user accounts with elevated privileges, or take further control of the affected system.

Impact

- Remote Code Execution
- Execution of arbitrary code in the user's context

- Compromise of confidentiality, integrity, and availability of the affected system

Solution/ Workarounds

Before installation of the software, please visit the vendor web-site for more details.

Apply the latest Microsoft Edge security update:

- Microsoft Edge 150.0.4078.48 or later.
- Enable automatic updates for Microsoft Edge.
- Instruct users to avoid opening untrusted links or attachments received through email or instant messaging.
- Restrict browsing to trusted websites where possible.

Reference

- Microsoft Security Update Guide: CVE-2026-58281

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.