May 17, 2024

Overall rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Microsoft has released an updated Edge Stable Channel. The vulnerability affects versions prior to version 124.0.2478.109

Technical Details

The high-severity zero-day vulnerability (CVE-2024-4947) is caused by a type confusion weakness, which has been reported by the Chromium team as having an exploit in the wild. Vulnerabilities of this type generally enable threat actors to trigger browser crashes by reading or writing memory out of buffer bounds, causing denial of service conditions, or possibly exploit them for arbitrary code execution on targeted devices.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk. ***This vulnerability is being exploited in the wild.***

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca.

References

- CVE-2024-4947
- Microsoft Edge Security Advisory
- VRM Vulnerability Reports