November 3, 2023

Overall rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Microsoft has released the latest Microsoft Edge (Chromium-based) Stable Channel. The vulnerability affects versions prior to 119.0.2151.44.

Technical Details

CVE-2023-36022 & CVE-2023-36034 are remote code execution vulnerabilities, that can be exploited by an unauthenticated, remote threat actor and execute remote commands on the affected versions of Microsoft Edge. However, According to Microsoft, this vulnerability requires user interaction to be performed before exploitation.

CVE-2023-36029 is a spoofing vulnerability that can be exploited by an unauthenticated attacker with network access, which requires certain user interactions to be performed. However, additional details about this vulnerability have not been published.

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

This vulnerability is rated as a **MEDIUM** risk. A software update exists to address this risk.

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.

References

- CVE-2023-36022, CVE-2023-36029, CVE-2023-36034
- Release notes for Microsoft Edge Security Updates
- VRM Vulnerability Reports