The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
11/22/2021

SUBJECT:
A Vulnerability in Microsoft Edge Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Microsoft Edge that could result in remote code execution. Microsoft Edge is a Chromium based internet browser made by Microsoft, which is installed by default on all new Windows computers. Edge was made to replace Internet Explorer, and runs faster and with more features. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Microsoft Edge cpe:/a:microsoft:edge DS
- Microsoft Windows 10 for 32-bit Systems
- Microsoft Windows 10 for x64-based Systems
- Microsoft Windows 10 version 1511 for 32-bit Systems
- Microsoft Windows 10 version 1511 for x64-based Systems
- Microsoft Windows 10 Version 1607 for 32-bit Systems
- Microsoft Windows 10 Version 1607 for x64-based Systems
- Microsoft Windows 10 version 1703 for 32-bit Systems
- Microsoft Windows 10 version 1703 for x64-based Systems
- Microsoft Windows 10 version 1709 for 32-bit Systems
- Microsoft Windows 10 version 1709 for x64-based Systems
- Microsoft Windows 10 Version 1803 for 32-bit Systems
- Microsoft Windows 10 Version 1803 for x64-based Systems
- Microsoft Windows Server 2016
- Microsoft Windows Server 2016 for x64-based Systems

RISK:

Government:

- Large and medium government entities: **High**
- Small government: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A design error vulnerability exists in Microsoft Edge (Chromium Based) which could allow for arbitrary code execution. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the security updates provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43221

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43221