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:
09/28/2021

SUBJECT:
Multiple Vulnerabilities in Microsoft Edge Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Edge, the most severe of which 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 the most severe of these vulnerabilities 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 of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
According to Google, an exploit for CVE-2021-37973 exists in the wild.

SYSTEMS AFFECTED:

- Microsoft Edge (Chromium-based) prior to 94.0.992.31

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:
Multiple vulnerabilities have been discovered in Microsoft Edge (Chromium Based), the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- Use after free vulnerability exists in Offline use. (CVE-2021-37956)
- Use after free vulnerability exists in WebGPU. (CVE-2021-37957)

- Inappropriate implementation vulnerability exists in Navigation. (CVE-2021-37958)
- Use after free vulnerability exists in Task Manager. (CVE-2021-37959)
- Inappropriate implementation vulnerability exists in Blink graphics. (CVE-2021-37960)
- Use after free vulnerability exists in Tab Strip. (CVE-2021-37961)
- Use after free vulnerability exists in Performance Manager. (CVE-2021-37962)
- Side-channel information leakage vulnerability exists in DevTools. (CVE-2021-37963)
- Inappropriate implementation vulnerability exists in ChromeOS Networking. (CVE-2021-37964)
- Inappropriate implementation vulnerability exists in Background Fetch API. (CVE-2021-37965)
- Inappropriate implementation vulnerability exists in Compositing. (CVE-2021-37966)
- Inappropriate implementation vulnerability exists in Background Fetch API. (CVE-2021-37967)
- Inappropriate implementation vulnerability exists in Background Fetch API. (CVE-2021-37968)
- Inappropriate implementation vulnerability exists in Google Updater. (CVE-2021-37969)
- Use after free vulnerability exists in File System API. (CVE-2021-37970)
- Incorrect security UI vulnerability exists in Web Browser UI. (CVE-2021-37971)
- Out of bounds read vulnerability exists in libjpeg-turbo. (CVE-2021-37972)
- Use after free vulnerability exists in Portals. (CVE-2021-37973)

Successful exploitation of the most severe of these vulnerabilities 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 of the most severe of these vulnerabilities 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/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37957
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37960

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37968
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37969
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37970
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37973

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.