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:
09/08/2021

SUBJECT:
A Vulnerability in Microsoft MSHTML Could Allow for Remote Code Execution.

OVERVIEW:
A vulnerability has been discovered in Microsoft MSHTML, which could allow for remote code execution. MSHTML (also known as Trident) is the engine used for Internet Explorer. It is also used by Microsoft Office applications for rendering web based content. Successful exploitation of this vulnerability could result in remote code execution in the context of the affected user. Depending on the privileges associated with the user, an attacker could view, change, or delete data.

THREAT INTELLIGENCE:
According to Microsoft, this threat is being exploited in the wild.

SYSTEMS AFFECTED:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows RT 8.1
- Windows 8.1
- Windows Server 2016
- Windows 10
- Windows Server, version 2004
- Windows Server 2022
- Windows Server 2019

RISK:
Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Microsoft MSHTML, which could allow for remote code execution. MSHTML (also known as Trident) is the engine used for Internet Explorer. It is also used by Microsoft Office applications for rendering web based content. Exploitation requires an attacker to craft a malicious Microsoft Office document that hosts the browser rendering engine, and entice a user to open it. Successful exploitation of this vulnerability could result in remote code execution in the context of the affected user. Depending on the privileges associated with the user, an attacker could view, change, or delete data.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- If patching is not possible, apply the appropriate work arounds as provided in the reference below.
- Run all software as a nonprivileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Microsoft:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40444

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.