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:
05/19/2021

SUBJECT:
A Vulnerability in Microsoft Windows JET Database Engine Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Microsoft Windows JET Database Engine that could allow for arbitrary code execution. Microsoft Windows JET Database Engine provides data access to various applications such as Microsoft Access, Microsoft Visual Basic, and third-party applications. Successful exploitation of this vulnerability could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

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

SYSTEMS AFFECTED:
- Microsoft Windows

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

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

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Microsoft Windows JET Database Engine that could allow for arbitrary code execution. This vulnerability can be exploited remotely if an attacker locates a vulnerable system. Microsoft Windows JET Database Engine is prone to a memory-corruption vulnerability because it fails to properly validate user-supplied data. An attacker can exploit this issue by enticing a victim to open specially crafted file or visit a specially crafted web

page. An attacker can exploit this issue to execute arbitrary code in the context of the current process. Successful exploitation of this vulnerability could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:
The following actions should be taken:

- 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:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8717

Zero Day Initiative:
https://www.zerodayinitiative.com/advisories/ZDI-21-594/

TLP: WHITE
https://www.cisa.gov/tlp