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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/09/2021

SUBJECT:
Critical Patches Issued for Microsoft Products, March 09, 2021

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are reports of two vulnerabilities observed being exploited in the wild (CVE-2021-27077 and CVE-2021-26411). CVE-2021-27077 is an Windows Win32k elevation of privilege vulnerability which allowed an attacker to escalate their privileges. CVE-2021-26411 is an Internet Explorer memory corruption vulnerability which would allow an attacker to run malicious code on the affected system when a user visited a specially crafted HTMl file. Proof-of-concept code is available for both of these CVEs.

SYSTEMS AFFECTED:
- Application Virtualization
- Azure
- Azure DevOps
- Azure Sphere
- Internet Explorer
- Microsoft ActiveX
- Microsoft Exchange Server
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office PowerPoint
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Windows Codecs Library

- Power BI
- Role: DNS Server
- Role: Hyper-V
- Visual Studio
- Visual Studio Code
- Windows Admin Center
- Windows Container Execution Agent
- Windows DirectX
- Windows Error Reporting
- Windows Event Tracing
- Windows Extensible Firmware Interface
- Windows Folder Redirection
- Windows Installer
- Windows Media
- Windows Overlay Filter
- Windows Print Spooler Components
- Windows Projected File System Filter Driver
- Windows Registry
- Windows Remote Access API
- Windows Storage Spaces Controller
- Windows Update Assistant
- Windows Update Stack
- Windows UPnP Device Host
- Windows User Profile Service
- Windows WalletService
- Windows Win32K

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

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

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution.

A full list of all vulnerabilities can be found at the link below:
https://msrc.microsoft.com/update-guide/en-us

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

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

REFERENCES:
Microsoft:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/releaseNote/2021-Mar

BleepingComputer:
https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2021-patch-tuesday-fixes-82-flaws-2-zero-days/