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:
12/14/2021

SUBJECT:
Critical Patches Issued for Microsoft Products, December 14, 2021

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution in the context of 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 currently reports of CVE-2021-43890 being exploited in the wild to spread malware such as Emotet, Trickbot, and Bazaloader.

SYSTEMS AFFECTED:

- Apps
- ASP.NET Core & Visual Studio
- Azure Bot Framework SDK
- BizTalk ESB Toolkit
- Internet Storage Name Service
- Microsoft Defender for IoT
- Microsoft Devices
- Microsoft Edge (Chromium-based)
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Message Queuing
- Microsoft Office
- Microsoft Office Access
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft PowerShell
- Microsoft Windows Codecs Library
- Office Developer Platform
- Remote Desktop Client
- Role: Windows Fax Service

- Role: Windows Hyper-V
- Visual Studio Code
- Visual Studio Code - WSL Extension
- Windows Common Log File System Driver
- Windows Digital TV Tuner
- Windows DirectX
- Windows Encrypting File System (EFS)
- Windows Event Tracing
- Windows Installer
- Windows Kernel
- Windows Media
- Windows Mobile Device Management
- Windows NTFS
- Windows Print Spooler Components
- Windows Remote Access Connection Manager
- Windows Storage
- Windows Storage Spaces Controller
- Windows SymCrypt
- Windows TCP/IP
- Windows Update Stack

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

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.

- Apply the Principle of Least Privilege to all systems and services, and 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/open files provided by unknown or untrusted sources.

REFERENCES:
Microsoft:

- https://msrc.microsoft.com/update-guide
- https://msrc.microsoft.com/update-guide/releaseNote/2021-Dec

ZDNet:

- https://www.zdnet.com/article/microsoft-december-2021-patch-tuesday-zero-day-exploited-to-spread-emotet-malware/