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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
04/12/2022

SUBJECT:
Critical Patches Issued for Microsoft Products, April 12, 2022

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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- .NET Framework
- Active Directory Domain Services
- Azure SDK
- Azure Site Recovery
- LDAP - Lightweight Directory Access Protocol
- Microsoft Bluetooth Driver
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Windows ALPC
- Microsoft Windows Codecs Library
- Microsoft Windows Media Foundation
- Power BI

- Role: DNS Server
- Role: Windows Hyper-V
- Skype for Business
- Visual Studio
- Visual Studio Code
- Windows Ancillary Function Driver for WinSock
- Windows App Store
- Windows AppX Package Manager
- Windows Cluster Client Failover
- Windows Cluster Shared Volume (CSV)
- Windows Common Log File System Driver
- Windows Defender
- Windows DWM Core Library
- Windows Endpoint Configuration Manager
- Windows Fax Compose Form
- Windows Feedback Hub
- Windows File Explorer
- Windows File Server
- Windows Installer
- Windows iSCSI Target Service
- Windows Kerberos
- Windows Kernel
- Windows Local Security Authority Subsystem Service
- Windows Media
- Windows Network File System
- Windows PowerShell
- Windows Print Spooler Components
- Windows RDP
- Windows Remote Procedure Call Runtime
- Windows schannel
- Windows SMB
- Windows Telephony Server
- Windows Upgrade Assistant
- Windows User Profile Service
- Windows Win32K
- Windows Work Folder Service
- YARP reverse proxy

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://learn.cisecurity.org/e/799323/update-guide/yqn13/293863943?h=N6ujtWB5G2yJClNn9qjTH54QznbpUpiwv3iihIoTHM8

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:
We recommend the following actions 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/2022-Apr