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:
01/11/2022

SUBJECT:
Critical Patches Issued for Microsoft Products, January 11, 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
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Teams
- Microsoft Windows Codecs Library
- Open Source Software
- Role: Windows Hyper-V
- Tablet Windows User Interface
- Windows Account Control
- Windows Active Directory
- Windows AppContracts API Server
- Windows Application Model
- Windows BackupKey Remote Protocol
- Windows Bind Filter Driver

- Windows Certificates
- Windows Cleanup Manager
- Windows Clipboard User Service
- Windows Cluster Port Driver
- Windows Common Log File System Driver
- Windows Connected Devices Platform Service
- Windows Cryptographic Services
- Windows Defender
- Windows Devices Human Interface
- Windows Diagnostic Hub
- Windows DirectX
- Windows DWM Core Library
- Windows Event Tracing
- Windows Geolocation Service
- Windows HTTP Protocol Stack
- Windows IKE Extension
- Windows Installer
- Windows Kerberos
- Windows Kernel
- Windows Libarchive
- Windows Local Security Authority
- Windows Local Security Authority Subsystem Service
- Windows Modern Execution Server
- Windows Push Notifications
- Windows RDP
- Windows Remote Access Connection Manager
- Windows Remote Desktop
- Windows Remote Procedure Call Runtime
- Windows Resilient File System (ReFS)
- Windows Secure Boot
- Windows Security Center
- Windows StateRepository API
- Windows Storage
- Windows Storage Spaces Controller
- Windows System Launcher
- Windows Task Flow Data Engine
- Windows Tile Data Repository
- Windows UEFI
- Windows UI Immersive Server
- Windows User Profile Service
- Windows User-mode Driver Framework
- Windows Virtual Machine IDE Drive
- Windows Win32K
- Windows Workstation Service Remote Protocol

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/2022-Jan

TLP: WHITE

https://www.cisa.gov/tlp