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:
07/13/2021

SUBJECT:
Critical Patches Issued for Microsoft Products, July 13, 2021

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for arbitrary 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 reports that the Windows Print Spooler Remote Code Execution Vulnerability (CVE-2021-34527), Windows Kernel Elevation of Privilege Vulnerabilities (CVE-2021-33771, CVE-2021-31979) and Scripting Engine Memory Corruption Vulnerability (CVE-2021-34448) are actively being exploited in the wild.

SYSTEMS AFFECTED:

- Common Internet File System
- Dynamics Business Central Control
- Microsoft Bing
- Microsoft Dynamics
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Scripting Engine
- Microsoft Windows Codecs Library
- Microsoft Windows DNS
- Microsoft Windows Media Foundation
- OpenEnclave
- Power BI

- Role: DNS Server
- Role: Hyper-V
- Visual Studio Code
- Visual Studio Code - .NET Runtime
- Visual Studio Code - Maven for Java Extension
- Windows Active Directory
- Windows Address Book
- Windows AF_UNIX Socket Provider
- Windows AppContainer
- Windows AppX Deployment Extensions
- Windows Authenticode
- Windows Cloud Files Mini Filter Driver
- Windows Console Driver
- Windows Defender
- Windows Desktop Bridge
- Windows Event Tracing
- Windows File History Service
- Windows Hello
- Windows HTML Platform
- Windows Installer
- Windows Kernel
- Windows Key Distribution Center
- Windows Local Security Authority Subsystem Service
- Windows MSHTML Platform
- Windows Partition Management Driver
- Windows PFX Encryption
- Windows Print Spooler Components
- Windows Projected File System
- Windows Remote Access Connection Manager
- Windows Remote Assistance
- Windows Secure Kernel Mode
- Windows Security Account Manager
- Windows Shell
- Windows SMB
- Windows Storage Spaces Controller
- Windows TCP/IP
- 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 arbitrary 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.
- 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://msrc.microsoft.com/update-guide
- https://msrc.microsoft.com/update-guide/releaseNote/2021-Jul

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.