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:
05/10/2022
05/11/2022 - UPDATED

SUBJECT:
Critical Patches Issued for Microsoft Products, May 10, 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.

May 11 – UPDATED SYSTEMS AFFECTED:
There are currently reports of CVE-2022-2692 being exploited in the wild.

SYSTEMS AFFECTED:

- .NET and Visual Studio
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Windows ALPC
- Remote Desktop Client
- Role: Windows Fax Service
- Role: Windows Hyper-V
- Self-hosted Integration Runtime
- Tablet Windows User Interface

- Visual Studio
- Visual Studio Code
- Windows Active Directory
- Windows Address Book
- Windows Authentication Methods
- Windows BitLocker
- Windows Cluster Shared Volume (CSV)
- Windows Failover Cluster Automation Server
- Windows Kerberos
- Windows Kernel
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Media
- Windows Network File System
- Windows NTFS
- Windows Point-to-Point Tunneling Protocol
- Windows Print Spooler Components
- Windows Push Notifications
- Windows Remote Access Connection Manager
- Windows Remote Desktop
- Windows Remote Procedure Call Runtime
- Windows Server Service
- Windows Storage Spaces Controller
- Windows WLAN Auto Config Service

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/241d1g/314694490?h=l8SUCwg6GafTHaSiPLJLUZ2GN7BbEWaEW4ErxMggapQ

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-May

May 11 – UPDATED REFERENCES:

HelpNetSecurity:

https://www.helpnetsecurity.com/2022/05/10/cve-2022-26925/