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:
04/13/2021 - **UPDATED**

SUBJECT:
UPDATED - Critical Patches Issued for Microsoft Products, April 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 no reports of these vulnerabilities being exploited in the wild.

April 13 – UPDATED THREAT INTELLIGENCE:

The following CVEs were disclosed publicly but are not known to be exploited in the wild:

- ***CVE-2021-27091 - RPC Endpoint Mapper Service Elevation of Privilege Vulnerability***
- ***CVE-2021-28312 - Windows NTFS Denial of Service Vulnerability***
- ***CVE-2021-28437 - Windows Installer Information Disclosure Vulnerability – PolarBear***
- ***CVE-2021-28458 - Azure ms-rest-nodeauth Library Elevation of Privilege Vulnerability***

CVE-2021-28310 (Win32k Elevation of Privilege Vulnerability) was discovered by Kaspersky and they are reporting that this vulnerability is possibly being exploited by the BITTER APT group.

SYSTEMS AFFECTED:

- Azure AD Web Sign-in
- Azure DevOps

- Azure Sphere
- Microsoft Edge (Chromium-based)
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Internet Messaging API
- Microsoft NTFS
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Windows Codecs Library
- Microsoft Windows Speech
- Open Source Software
- Role: DNS Server
- Role: Hyper-V
- Visual Studio
- Visual Studio Code
- Visual Studio Code - GitHub Pull Requests and Issues Extension
- Visual Studio Code - Kubernetes Tools
- Visual Studio Code - Maven for Java Extension
- Windows Application Compatibility Cache
- Windows AppX Deployment Extensions
- Windows Console Driver
- Windows Diagnostic Hub
- Windows Early Launch Antimalware Driver
- Windows ELAM
- Windows Event Tracing
- Windows Installer
- Windows Kernel
- Windows Media Player
- Windows Network File System
- Windows Overlay Filter
- Windows Portmapping
- Windows Registry
- Windows Remote Procedure Call Runtime
- Windows Resource Manager
- Windows Secure Kernel Mode
- Windows Services and Controller App
- Windows SMB Server
- Windows TCP/IP
- Windows Win32K
- 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 arbitrary code execution.

A full list of all vulnerabilities can be found at the link below:
https://msrc.microsoft.com/update-guide/en-us

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-Apr

April 13 – UPDATED REFERENCES:
Bleeping Computer:
https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2021-patch-tuesday-fixes-108-flaws-5-zero-days/

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.