*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**
**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**
**http://www.us-cert.gov/tlp/**

**DATE(S) ISSUED:**
02/09/2021

**SUBJECT:**
Critical Patches Issued for Microsoft Products, February 09, 2021

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution. 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.

**THREAT INTELLIGENCE:**
The Windows Win32k Elevation of Privilege Vulnerability (CVE-2021-1732), which allows an attacker or malicious program to elevate their privileges to administrative privileges, has been seen exploited in the wild. In addition the Package Managers Configurations Remote Code Execution Vulnerability (CVE-2021-24105) has a proof of concept, which is available to the public.

**SYSTEMS AFFECTED:**
- .NET Core
- .NET Framework
- Azure IoT
- Developer Tools
- Microsoft Azure Kubernetes Service
- Microsoft Dynamics
- Microsoft Edge for Android
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Windows Codecs Library
- Role: DNS Server
- Role: Hyper-V
- Role: Windows Fax Service
- Skype for Business

- SysInternals
- System Center
- Visual Studio
- Windows Address Book
- Windows Backup Engine
- Windows Console Driver
- Windows Defender
- Windows DirectX
- Windows Event Tracing
- Windows Installer
- Windows Kernel
- Windows Mobile Device Management
- Windows Network File System
- Windows PFX Encryption
- Windows PKU2U
- Windows PowerShell
- Windows Print Spooler Components
- Windows Remote Procedure Call
- Windows TCP/IP
- Windows Trust Verification API

**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/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://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24105

**Bleeping Computer:**
https://www.bleepingcomputer.com/news/security/microsoft-february-2021-patch-tuesday-fixes-56-flaws-1-zero-day/