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:
06/08/2021
06/08/2021 – *UPDATED*
06/30/2021 – UPDATED

SUBJECT:
Critical Patches Issued for Microsoft Products, June 8, 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.

June 8 – UPDATED THREAT INTELLIGENCE:
There are six zero-day vulnerabilities that Microsoft has tracked as being actively exploited which include CVE-2021-33742, CVE-2021-33739, CVE-2021-31199, CVE-2021-31201, CVE-2021-31955 and CVE-2021-31956.

June 30 – UPDATED THREAT INTELLIENCE:
Researchers have proved that CVE-2021-1675 can be exploited to achieve remote code execution and proof of concept exploits have since been leaked. There are reports that the patch for CVE-2021-1675 is not enough to foil the zero-day PoC available.

SYSTEMS AFFECTED:

- .NET Core & Visual Studio
- 3D Viewer
- Microsoft DWM Core Library
- Microsoft Intune
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Office SharePoint

- Microsoft Scripting Engine
- Microsoft Windows Codecs Library
- Paint 3D
- Role: Hyper-V
- Visual Studio Code - Kubernetes Tools
- Windows Bind Filter Driver
- Windows Common Log File System Driver
- Windows Cryptographic Services
- Windows DCOM Server
- Windows Defender
- Windows Drivers
- Windows Event Logging Service
- Windows Filter Manager
- Windows HTML Platform
- Windows Installer
- Windows Kerberos
- Windows Kernel
- Windows Kernel-Mode Drivers
- Windows Network File System
- Windows NTFS
- Windows NTLM
- Windows Print Spooler Components
- Windows Remote Desktop
- Windows TCP/IP

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.

June 30 – UPDATED RECOMMENDATIONS:
We recommend the following actions be taken:

- ***Disable the "Print Spooler" service on machines that don't require it.***

REFERENCES:
Microsoft:

- https://msrc.microsoft.com/update-guide
- https://msrc.microsoft.com/update-guide/releaseNote/2021-Jun

June 8 – UPDATED REFERENCES:
ZDNet:

- *https://www.zdnet.com/article/microsoft-june-2021-patch-tuesday-50-vulnerabilities-patched-including-six-zero-days-exploited-in-the-wild/*

June 30 – UPDATED REFERENCES:
HelpNetSecurity:

- ***https://www.helpnetsecurity.com/2021/06/30/poc-cve-2021-1675/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29***

Tenable:

- ***https://www.tenable.com/blog/cve-2021-1675-proof-of-concept-leaked-for-critical-windows-print-spooler-vulnerability***

Threatpost:

- ***https://threatpost.com/poc-exploit-windows-print-spooler-bug/167430/***

Twitter:

- ***https://twitter.com/wdormann/status/1410198834970599425***
- ***https://twitter.com/hackerfantastic/status/1410100394492112898?ref_src=twsrc%5Etfw***

Microsoft:

- ***https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675***

Redmond:

- ***https://redmondmag.com/articles/2021/06/30/microsoft-print-spool-patch.aspx***