

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:

09/14/2021

SUBJECT:

Critical Patches Issued for Microsoft Products, September 14, 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.

SYSTEMS AFFECTED:

- Azure Open Management Infrastructure
- Azure Sphere
- Dynamics Business Central Control
- Microsoft Accessibility Insights for Android
- Microsoft Edge (Chromium-based)
- Microsoft Edge for Android
- Microsoft MPEG-2 Video Extension
- Microsoft Office
- Microsoft Office Access
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Office Word
- Microsoft Windows Codecs Library
- Microsoft Windows DNS
- Visual Studio
- Windows Ancillary Function Driver for WinSock
- Windows Authenticode

- Windows Bind Filter Driver
- Windows BitLocker
- Windows Common Log File System Driver
- Windows Event Tracing
- Windows Installer
- Windows Kernel
- Windows Key Storage Provider
- Windows MSHTML Platform
- Windows Print Spooler Components
- Windows Redirected Drive Buffering
- Windows Scripting
- Windows SMB
- Windows Storage
- Windows Subsystem for Linux
- Windows TDX.sys
- Windows Update
- Windows Win32K
- Windows WLAN Auto Config Service
- Windows WLAN 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>

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-Sep>

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.