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:
05/11/2021

08/23/2021 - **UPDATED**

SUBJECT:
Critical Patches Issued for Microsoft Products, May 11, 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.

August 23 – UPDATED THREAT INTELLIGENCE:

According to open source research, the following CVEs are actively being exploited in the wild through the ProxyShell vulnerabilities:

CVE-2021-31207 (Post-Authentication Arbitrary File Write, May 2021)

CVE-2021-34473 (Pre-Authentication Path Confusion, July 2021)

CVE-2021-34523 (Exchange PowerShell Backend Elevation of Privilege, July 2021)

SYSTEMS AFFECTED:

- .NET Core & Visual Studio
- HTTP.sys
- Internet Explorer
- Microsoft Accessibility Insights for Web
- Microsoft Bluetooth Driver
- Microsoft Dynamics Finance & Operations
- Microsoft Exchange Server
- Microsoft Graphics Component

- Microsoft Office
- Microsoft Office Access
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft Windows Codecs Library
- Microsoft Windows IrDA
- Open Source Software
- Role: Hyper-V
- Skype for Business and Microsoft Lync
- Visual Studio
- Visual Studio Code
- Windows Container Isolation FS Filter Driver
- Windows Container Manager Service
- Windows Cryptographic Services
- Windows CSC Service
- Windows Desktop Bridge
- Windows OLE
- Windows Projected File System FS Filter
- Windows RDP Client
- Windows SMB
- Windows SSDP Service
- Windows WalletService
- Windows Wireless Networking

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.

UPDATED RECOMMENDATIONS:

- ***We recommend you update to the latest Microsoft Exchange security patch, monitor for new indicators of compromise and stay up-to-date on new information as it is released***

REFERENCES:

Microsoft:

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

August 23 – UPDATED REFERENCES:

Huntress Labs:

- ***https://www.huntress.com/blog/rapid-response-microsoft-exchange-servers-still-vulnerable-to-proxyshell-exploit***

Tech Community:

- ***https://techcommunity.microsoft.com/t5/exchange-team-blog/released-may-2021-exchange-server-security-updates/ba-p/2335209***

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.