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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

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:
10/11/2022

SUBJECT:
Critical Patches Issued for Microsoft Products, October 11, 2022

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote 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:
Two zero-day vulnerabilities, CVE-2022-41043 (Microsoft Office Information Disclosure Vulnerability) which has been reported by Microsoft as currently being exploited in the wild and CVE-2022-41033 (Windows COM+ Event System Service Elevation of Privilege Vulnerability) which has not been reported by Microsoft as currently being exploited in the wild, have both been fixed in the latest patch.

Meanwhile, Microsoft has not released security updates for two actively exploited zero-day vulnerabilities tracked as CVE-2022-41040 and CVE-2022-41082, also known as ProxyNotShell. There are multiple reports detailing the active exploitation of these vulnerabilities, which includes security researchers tracking active campaigns leveraging remote code execution vulnerabilities. GTSC, the Vietnamese cybersecurity company that discovered the two vulnerabilities, reported the vulnerabilities were exploited in early August 2022. According to the GTSC report, cyber threat actors (CTAs) are chaining the vulnerabilities to create backdoors for persistence or to move laterally in the victim network. For example, CTAs exploiting these vulnerabilities

deployed the China Chopper webshell for persistent remote access. Some security researchers are referring to the exploit chain as “ProxyNotShell.”

Researchers have warned that Microsoft's mitigation can be bypassed. Security researcher Jang documented how a potential attacker could bypass the proposed mitigation with little effort, and researchers at GTSC confirmed the bypass. However, please note Microsoft has released updated mitigations as of 10/7 and the aforementioned bypass was reported prior. Researchers have also warned that users with a hybrid setup combining on-premises and cloud deployment of exchange are also vulnerable to these zero days.

A BleepingComputer report noted that a scammer set up a GitHub repository and is “impersonating security researchers to sell fake proof-of-concept ProxyNotShell exploits” for Exchange CVE-2022-41040 and CVE-2022-41082 vulnerabilities.

CISA is aware of the vulnerabilities and encourages users and administrators to review information from Microsoft and “apply the necessary mitigations until patches are made available.”

SYSTEMS AFFECTED:

- Active Directory Domain Services
- Azure
- Azure Arc
- Client Server Run-time Subsystem (CSRSS)
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Word
- Microsoft WDAC OLE DB provider for SQL
- NuGet Client
- Remote Access Service Point-to-Point Tunneling Protocol
- Role: Windows Hyper-V
- Service Fabric
- Visual Studio Code
- Windows Active Directory Certificate Services
- Windows ALPC
- Windows CD-ROM Driver
- Windows COM+ Event System Service
- Windows Connected User Experiences and Telemetry
- Windows CryptoAPI
- Windows Defender
- Windows DHCP Client
- Windows Distributed File System (DFS)

- Windows DWM Core Library
- Windows Event Logging Service
- Windows Group Policy
- Windows Group Policy Preference Client
- Windows Internet Key Exchange (IKE) Protocol
- Windows Kernel
- Windows Local Security Authority (LSA)
- Windows Local Security Authority Subsystem Service (LSASS)
- Windows Local Session Manager (LSM)
- Windows NTFS
- Windows NTLM
- Windows ODBC Driver
- Windows Perception Simulation Service
- Windows Point-to-Point Tunneling Protocol
- Windows Portable Device Enumerator Service
- Windows Print Spooler Components
- Windows Resilient File System (ReFS)
- Windows Secure Channel
- Windows Security Support Provider Interface
- Windows Server Remotely Accessible Registry Keys
- Windows Server Service
- Windows Storage
- Windows TCP/IP
- Windows USB Serial Driver
- Windows Web Account Manager
- Windows Win32K
- Windows WLAN Service
- Windows Workstation 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 remote code execution.

A full list of all vulnerabilities can be found at the link below:
https://learn.cisecurity.org/e/799323/update-guide/3xxmgn/513754735?h=eo9PW4vupV5uYoOE8MzGJtz2vgPYk5eZrd6rdEf2-hc

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:
We recommend the following actions be taken:

- For CVE-2022-41040 and CVE-2022-41082: Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries (**M1042**: Disable or Remove Feature or Program)
    - **Safeguard 4.8 : Uninstall or Disable Unnecessary Services on Enterprise Assets and Software:** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.
- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Apply the Principle of Least Privilege to all systems and services, and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Remind all users not to visit untrusted websites or follow links/open files provided by unknown or untrusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES:

Microsoft:

- https://msrc.microsoft.com/update-guide/
- https://msrc.microsoft.com/update-guide/releaseNote/2022-Oct
- https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/ **(CVE-2022-41040 and CVE-2022-41082 Updated Mitigations)**