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.

DATE(S) ISSUED:
09/30/2022

SUBJECT:
Multiple Vulnerabilities in Microsoft Exchange Server Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Exchange Server, the most severe of which could allow for remote code execution. Microsoft Exchange Server is a mail server used to run and manage an organization's email services. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the affected service account. Depending on the privileges associated with the account an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Service accounts that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

THREAT INTELLIGENCE:
At this time, Microsoft is aware of limited targeted attacks using the vulnerabilities to access systems.

SYSTEMS AFFECTED:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

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 Exchange Server, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

Tactic: *Lateral Movement* (TA0008):

Technique: *Exploitation of Remote Services* (T1210):

- CVE-2022-41040 – Microsoft Exchange Server Server-Side Request Forgery (SSRF) vulnerability
- CVE-2022-41082 – Microsoft Exchange Server Remote Code execution vulnerability

In order to successfully exploit the SSRF vulnerability CVE-2022-41040, authentication to the exchange server is required. If CVE-2022-41040 is successfully exploited, it may be chained with CVE-2022-41082 to allow for remote code execution by accessing the PowerShell Remoting Service (default ports 5985/TCP and 5986/TCP).

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the affected service account. Depending on the privileges associated with the account an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Service accounts that 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:

- Apply the workarounds provided by Microsoft (link below) until a patch is available. When available, apply appropriate updates 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. Run all software as a non-privileged user (one without administrative privileges) 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.
    - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
    - **Safeguard 6.8: Define and Maintain Role-Based Access Control:** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.
    - **Safeguard 13.10: Performing Application Layer Filtering:** Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

REFERENCES:

Microsoft:

https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082