TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2021-030

DATE(S) ISSUED:
03/02/2021

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Exchange Server (on premises version) , the most severe of which could allow for arbitrary 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 an attacker to execute arbitrary code in the context of the mail server. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
Microsoft has detected the threat actor HAFNIUM exploiting these vulnerabilities. HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. For more information on this threat actor and the details of the observed attacks please visit the Microsoft URL in the reference section.

SYSTEMS AFFECTED:
- Microsoft Exchange Server 2010 RU31 for Service Pack 3
- Microsoft Exchange Server 2013 CU 23
- Microsoft Exchange Server 2016 CU 18, CU 19
- Microsoft Exchange Server 2019 CU 7, CU 8

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Exchange Server, the most severe of which could allow for arbitrary code execution. These vulnerabilities can be exploited remotely if an attacker locates a vulnerable server. Details of the vulnerabilities are as follows:

- A server-side request forgery (SSRF) vulnerability in Exchange which allows the attacker to send arbitrary HTTP requests and authenticate as the Exchange server. [CVE-2021-26855]
- An insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is deserialized by a program. Exploiting this vulnerability gives an the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to exploit. [CVE-2021-26857]
- A post-authentication arbitrary file write vulnerability in Exchange. If an attacker could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials. [CVE-2021-26858]
- A post-authentication arbitrary file write vulnerability in Exchange. If an attacker could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials. [CVE-2021-27065]

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the mail server. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply the stable channel update provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Microsoft:
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Microsoft Security Response Center:
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26855
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26857
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27065

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/