**TLP: WHITE**
**MS-ISAC CYBERSECURITY ADVISORY**

**MS-ISAC ADVISORY NUMBER:** 2019-011

**DATE(S) ISSUED:** 01/29/2019

**SUBJECT:** A Vulnerability in Microsoft Exchange Could Allow for Privilege Escalation.

**OVERVIEW:**
A vulnerability has been discovered in Microsoft Exchange which could allow for privilege escalation. Microsoft Exchange is an email server available for Microsoft Windows. Successful exploitation of this vulnerability could allow for privilege escalation to the Domain Admin account. Access to the Domain Admin account could allow for an attacker to perform a series of malicious actions including the ability implement backdoor accounts on the system.

**THREAT INTELLIGENCE:**
A Proof-of-Concept has been developed by the researchers who discovered this vulnerability to demonstrate this issue.

**SYSTEMS AFFECTED:**
- Microsoft Exchange 2013 and newer

**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:**
A vulnerability has been discovered in Microsoft Exchange, which could allow for privilege escalation. In the context of any compromised email account on the network, an attacker may be able to gain access to the Domain Admin account due to default configuration settings on Microsoft Exchange Servers. It is also possible to perform this attack without any credentials. An attacker may achieve this due to the following:

1. Exchange Servers by default are configured with many high privilege operations, this includes write access to the Domain Object in Active Directory. Access to Domain Object enables the user to modify domain privileges.
2. Exchange Servers are vulnerable to NTLM relay attacks because the Exchange server fails to set the Sign and Seal flags on NTLM operations. This can allow attackers to obtain the server's NTML hash.
3. A feature in Exchange Web Services (EWS) can allow attackers to trick the Exchange Server authenticate on an attacker-controlled URL over HTTP using the server's computer account.
4. If the attacker does not have credentials, it is possible to still trigger Exchange to authenticate to an attacker controlled URL by performing a SMB to HTTP relay attack.

Successful exploitation of this vulnerability could allow for privilege escalation to the Domain Admin account. Access to the Domain Admin account could allow for an attacker to perform a series of malicious actions including the ability implement backdoor accounts on the system.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Consider implementing mitigation recommendations for this vulnerability found at the reference link below.
- Apply appropriate patch provided by Microsoft, once available, after appropriate testing.
- 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:**

**Proof of Concept:**
https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin

**Mitigations:**
**Carnegie Melon CERT:**
https://kb.cert.org/vuls/id/465632/

24×7 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