RISA
Rwanda Information Society Authority

Rw CSIRT
Computer Security & Incident Response Team

Alert – A Vulnerability in Microsoft Exchange

Description:

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.

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:

Microsoft Exchange supports a API called **Exchange Web Services (EWS).** One of the EWS API functions is called **PushSubscriptionRequest**, which can be used to cause the Exchange server to connect to an arbitrary website. Connections made using the PushSubscriptionRequest function will attempt to negotiate with the arbitrary web server using NTLM authentication. Microsoft Exchange is by default configured with extensive privileges with respect to the Domain object in Active Directory. Because the Exchange Windows Permissions group has WriteDacl access to the Domain object, this means that the Exchange server privileges obtained using this vulnerability can be used to gain Domain Admin privileges for the domain that contains the vulnerable Exchange server. An attacker may achieve this due to the following:

- 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.
- 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.. in other words, starting with Microsoft Exchange 2013, the NTLM authentication over HTTP fails to set the NTLM Sign and Seal flags. The lack of signing makes this authentication attempt vulnerable to NTLM relay attacks and which can allow a remote attacker to gain the privileges of the Exchange server.

- 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.
- 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.

Solution (Mitigations):

Rw-CSIRT is strongly recommending **users** and **IT administrators** to:

- Consider implementing mitigation recommendations for this vulnerability found at the reference links 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, in other words, remove the unnecessary high privileges that Exchange has on the Domain object (see below for some links on this).
- Enable LDAP signing and **enable LDAP channel binding** to prevent relaying to LDAP and LDAPS respectively
- Block Exchange servers from making connections to workstations on arbitrary ports.
- Enable **Extended Protection for Authentication** on the Exchange endpoints in IIS (but not the Exchange Back End ones, this will break Exchange). This will verify the channel binding parameters in the NTLM authentication, which ties NTLM authentication to a TLS connection and prevent relaying to Exchange web services.
- Remove the registry key which makes relaying back to the Exchange server possible, as discussed in Microsofts **mitigation for CVE-2018-8518.**
- Enforce SMB signing on Exchange servers (and preferable all other servers and workstations in the domain) to prevent cross-protocol relay attacks to SMB.
- If EWS push/pull subscriptions aren't used, they can be disabled by setting the EWSMaxSubscriptions to 0 with a **throttling policy**, (after testing it)

Affected users should: contact RW-CSIRT: Call **4045** or write to **security@risa.rw** to help for analyzing the source of the incident and recommendation.

References:

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

Mitigations:
https://kb.cert.org/vuls/id/465632/

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of: "early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability" and raise cyber security awareness in public.