


Advanced Notification of Cyber Threats against Microsoft Exchange Privilege Elevation Vulnerability



Security Advisory ADV-19-04 **Criticality** High 

Advisory Released On 07 February 2019

Impact

A vulnerability in Microsoft Exchange that could be exploited to permit privilege elevation of an Exchange user into a domain admin.

Solution

[Adhere the advices written under the recommendations section.](#)

Affected Platforms

- Microsoft Exchange Server

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a newly discovered vulnerability currently named as “Microsoft Exchange Server Elevation of Privilege Vulnerability”, with CVE ID of “CVE-2018-8581”. This vulnerability can be exploited by executing a man-in-the-middle attack. Successful exploitation could result in the attacker to attempt impersonating any user of the Exchange server and elevate into a domain admin.

Threat Details

Microsoft Exchange Privilege Elevation Vulnerability may escalate any user with a mailbox in the Exchange server into a Domain Admin. Successful exploitation is done via impersonating Exchange user by the execution of a man-in-the-middle attack. As mentioned earlier, any user with a mailbox after exploiting the vulnerability may elevate into a Domain Admin. Thereby, Domain Admin elevation may permit attackers to perform a series of various malicious activities and the implementation of backdoor on the targeted systems.

Any compromised Exchange user with a mailbox can be exploited by attackers, then be used to elevate into a Domain Admin. Moreover, it is also possible to exploit this vulnerability and gain Domain Admin even without a compromised Exchange user and without any credentials.

Furthermore, patches are currently not available, at the date of Advisory release February 7, 2019, and this vulnerability is possible by default in Exchange Server.

For reasons such as:

- The privileges of Exchange Servers are high by default.
- Exchange Servers make use of NTLM authentication, which is currently vulnerable to relay attacks.
- Exchange currently authenticates attackers with the computer account of Exchange server.

Recommendations

To mitigate against the vulnerability, entities are recommended with the following:

1. Apply patches as soon as they are available.
2. Remove unnecessary high privileges that Exchange has on the Domain.
3. Block Exchange connections to workstations on random ports.
4. Prevent relaying of LDAP and LDAPS by enabling LDAP signing and LDAP channel binding.
5. Prevent cross-protocol replay attack to SMB by enforcing SMB signing on Exchange servers.
6. Remove registry key that enables relaying back to Exchange servers
 - a. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

References

[Microsoft Security TechCenter](#)

[CIS Center for Internet Security](#)

<https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/>

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email [info\[at\]aeCERT.ae](mailto:info[at]aeCERT.ae)
Instagram [@TheUAETRA](#)
Twitter [@TheUAETRA](#)

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to [aeCERT\[at\]aeCERT.ae](mailto:aeCERT[at]aeCERT.ae)