Security Advisory 2021-019

New Critical Vulnerabilities in Microsoft Exchange Server

April 14, 2021 — v1.0

TLP:WHITE

Summary

On the 13th of April 2021, Microsoft released a software update to mitigate critical vulnerabilities that affect on-premises Exchange Servers 2013, 2016, and 2019 [1, 2, 3, 4]. An attacker could use these vulnerabilities to gain access and maintain persistence on the target host. These new vulnerabilities are different from the ones disclosed and fixed in March 2021, therefore the security updates released in March 2021 will not remediate against these vulnerabilities.

No active exploitation of these vulnerabilities is known yet, however, because of the increased impact of the vulnerabilities and the fact that the amount of potentially sensitive information that is stored in Exchange servers, it is highly recommended to **apply the patches as soon as possible** [5].

Technical Details

All five vulnerabilities have the same descriptions by Microsoft, however Tenable provided technical analysis for CVE-2021-26877 and CVE-2021-26897 [6].

The vulnerabilities CVE-2021-28480 and CVE-2021-28481 are pre-authentication vulnerabilities in Microsoft Exchange Server. A pre-authentication vulnerability means that an attacker does not need to authenticate to the vulnerable Exchange Server in order to exploit the vulnerability. All the attacker needs to do, is to perform reconnaissance against their intended targets and then send specially crafted requests to the vulnerable Exchange Server.

The vulnerabilities CVE-2021-28482 and CVE-2021-28483 are post-authentication vulnerabilities in Microsoft Exchange Server. Unlike CVE-2021-28480 and CVE-2021-28481, these are only exploitable once an attacker has authenticated to a vulnerable Exchange Server. However, these flaws could be chained together with a pre-authentication Exchange Server vulnerability to bypass that requirement.

Affected Products

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

To be exploitable, Microsoft Exchange Servers have to be on-premises versions of Microsoft Exchange Server. Microsoft Exchange Online is not affected by these flaws. Microsoft says Exchange Server 2010 is also not affected by these new vulnerabilities.

Recommendations

Applying the update released on April 13 to Exchange servers [5] is currently the only mitigation for these vulnerabilities (aside from removing affected servers from the network).

References

[1] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28480

[2] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28481

[3] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28482

[4] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-28483

[5] https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-april-13-2021-kb5001779-8e08f3b3-fc7b-466c-bbb7-5d5aa16ef064

[6] https://www.tenable.com/blog/cve-2021-28480-cve-2021-28481-cve-2021-28482-cve-2021-28483-four-critical-microsoft-exchange