Security Advisory 2022-015

Critical Vulnerability in Microsoft Exchange Server

March 10, 2022 — v1.0

TLP:WHITE

History:

- *10/03/2022 — v1.0 – Initial publication*

Summary

On March 8th, Microsoft issued the monthly Patch Tuesday where 71 vulnerabilities were fixed. Three of them were classified as **Critical** as they allow remote code execution (RCE) [1]. One of these critical vulnerabilities affects Microsoft Exchange Server.

The vulnerability tracked as CVE-2022-23277 is a remote code execution vulnerability that can be exploited by an authenticated attacker to perfom RCE on Microsoft Exchange [2]. No active exploitation of this vulnerability is known yet.

Technical Details

There is not much detail available about how this vulnerability could be exploited. As per Microsoft, the attacker exploiting this vulnerability could target the server accounts for an arbitrary or remote code execution. As an authenticated user, the attacker could attempt to trigger malicious code in the context of the server's account through a network call [2].

Affected Products

- Microsoft Exchange Server 2019 Cumulative Update 11
- Microsoft Exchange Server 2019 Cumulative Update 10
- Microsoft Exchange Server 2016 Cumulative Update 22
- Microsoft Exchange Server 2016 Cumulative Update 21
- Microsoft Exchange Server 2013 Cumulative Update 23

Recommendations

Given the fact that we have observed increasing attacks against Microsoft Exchange, we strongly advise to apply the patch as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2022-patch-tuesday-fixes-71-flaws-3-zero-days/

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23277