CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-063

RCE Vulnerability in Microsoft Exchange Server

November 10, 2021 — v1.0

TLP:WHITE

History:

- *10/11/2021 — v1.0 – Initial publication*

Summary

On November 9, Microsoft released Exchange Server Security Updates fixing several vulnerabilities [1], one of which identified as `CVE-2021-42321` has a CVSS3.1 score of 8.8 out of 10 [2]. This is a post-authentication vulnerability that could allow an attacker to execute remote code on Exchange 2016 and 2019.

This vulnerability affects on-premises Microsoft Exchange Server, including servers used in Exchange Hybrid mode. Exchange Online customers are already protected and do not need to take any action.

Microsoft is aware of limited targeted attacks by using this vulnerability. CERT-EU recommendation is to install these updates immediately [2].

Technical Details

There is not much detail available about the vulnerability `CVE-2021-42321` [2]. According to Redmond's security advisory, it is caused by improper validation of `cmdlet` arguments. However, attackers must be authenticated.

Affected Products

- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016

To be exploitable, Microsoft Exchange Servers have to be *on-premise* versions of Microsoft Exchange Server, including servers used in Exchange Hybrid mode. Microsoft Exchange Online is not affected by these flaws.

Recommendations

Applying the updates released on November 9 to Exchange servers [2] is currently the only mitigation for this vulnerability:

- Exchange Server 2016 CU21 and CU22
- Exchange Server 2019 CU10 and CU11

In order to see if an exploit was attempted, run the following PowerShell query on your Exchange server to check for specific events in the Event Log:

```
Get-EventLog -LogName Application -Source "MSExchange Common" -EntryType Error | Where-Object {
   $_.Message -like "*BinaryFormatter.Deserialize*" }
```

References

[1] https://techcommunity.microsoft.com/t5/exchange-team-blog/released-november-2021-exchange-server-security-updates/ba-p/2933169

[2] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321