CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-013

Zero-Day Vulnerabilities in Microsoft Exchange

March 16, 2021 — v1.2

TLP:WHITE

History:

- *03/03/2021 — v1.0 – Initial publication*
- *11/03/2021 — v1.1 – Update concerning recommended investigation*
- *16/03/2021 — v1.2 – Update concerning Microsoft mitigation tool*

Summary

Several Zero Day vulnerabilities affecting Microsoft Exchange servers were observed exploited in the wild [1]. Vulnerabilities are critical, so it is extremely important to **apply the patches as soon as possible** [2].

It has been confirmed that the attacks have started before the patch was available and **thousands** of Exchange installation have been compromised. At this stage, simply patching is **not sufficient**. Proper investigation has to be performed to asses the **potential compromise**.

Microsoft has now released a mitigation tool that can help security teams [7].

Technical Details

Microsoft Exchange vulnerabilities were used to steal e-mails and compromise networks:

- **CVE-2021-26855** – a server-side request forgery (SSRF) vulnerability in Exchange which allows the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
- **CVE-2021-26857** – an insecure deserialisation vulnerability in the Unified Messaging service. Insecure deserialisation is where untrusted user-controllable data is deserialised by a program. Exploiting this vulnerability gives attackers the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to exploit.
- **CVE-2021-26858** – a post-authentication arbitrary file write vulnerability in Exchange. When authenticated, the attackers can use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate Administrator credentials.
- **CVE-2021-27065** – a post-authentication arbitrary file write vulnerability in Exchange. This vulnerability can be used to write a file to any path on the server.

As part of an incident investigation, exploitation of these vulnerabilities was observed starting at least 6th of January 2021. We are not aware of publicly available code to exploit these Exchange vulnerabilities, but given the exposure it may arise soon.

Affected Products

- Microsoft Exchange Server 2013, 2016 and 2019.

Exchange Online service is not affected.

Recommendations

Apply the patches as soon as possible [2]. It is recommended to prioritise the updates on Internet-facing Exchange Servers.

Even for patched, on-premises servers that are (or were) exposing to Internet any other services than SMTP (such as OWA or ActiveSync), we recommend performing the following checks:

- Perform the checks mentioned in the Microsoft paper on your Exchange server [4].
- Scan Exchange server with Microsoft detection tool [5].
- Check your logs for the IoCs mentioned in [6].

Mitigation

This vulnerability is part of an attack chain. The initial attack requires the ability to make an untrusted connection to Exchange server port 443. This can be protected against by restricting untrusted connections, or by setting up a VPN to separate the Exchange server from external access. Using this mitigation will only protect against the initial portion of the attack. Other portions of the chain can still be triggered if an attacker already has access or can convince an administrator to open a malicious file.

To help quickly protect the Exchange environments, Microsoft produced an additional series of security updates (SUs) that can be applied to some older (and unsupported) Cumulative Updates (CUs). This is intended only as a temporary measure to help protect vulnerable machines right now. You still need to update to the latest supported CU and then apply the applicable SUs [3].

Microsoft has released recently a tool that checks if the server is vulnerable, mitigates CVE-2021-26855, downloads and runs the Microsoft Safety Scanner in order to remove any malicious files found [7].

References

[1] https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

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

[3] https://techcommunity.microsoft.com/t5/exchange-team-blog/march-2021-exchange-server-security-updates-for-older-cumulative/ba-p/2192020

[4] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[5] https://www.bleepingcomputer.com/news/security/microsofts-msert-tool-now-finds-web-shells-from-exchange-server-attacks/

[6] https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

[7] https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-one-click-exchange-on-premises-mitigation-tool/