Does ESET provide protection against attacks leveraging the recent Microsoft Exchange vulnerabilities

2021-03-10 - Mitchell | ESET Nederland - Comments (0) - Customer Advisories

Summary

On March 2, 2021, Microsoft released information about critical vulnerabilities in its Exchange Server 2013, 2016, and 2019. These vulnerabilities allow a remote attacker to take control over any Exchange server that is reachable via the internet, without knowing any access credentials. At the same time, Microsoft also released patches for these vulnerabilities and ESET strongly advises to install them as soon as possible.

Details

The vulnerabilities were initially reported to Microsoft on January 5, 2021. However, reports claim they were exploited in-the-wild as soon as January 3, 2021. ESET has detected that more than 5000 servers around the world have already been compromised by various attackers, predominantly APT (advanced persistent threat) groups.

The nature of the vulnerabilities allows the installation of a webshell to the server, which can then serve as an entry point for further malware installation. ESET Security products detect the following webshells and backdoors used in the exploitation process:

- JS/Exploit.CVE-2021-26855.Webshell.A
- JS/Exploit.CVE-2021-26855.Webshell.B
- ASP/Webshell
- ASP/ReGeorg

Given the high level of exploitability and the fact that multiple threat actors are actively scanning the internet to find exploitable servers, it is expected that most servers open to the internet could have been compromised. In order to prevent further exploitation, it is necessary to install the available updates provided by Microsoft as soon as possible.

However, applying the patches does not clean already breached servers. It is, therefore, necessary to perform an investigation and search for compromise remnants and malware or malware traces in the environment, as well as change the access credentials.

For further in-depth analysis and details on remediation of a compromised server, please refer to ESET's WeLiveSecurity blog post at https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/.

Note: One of the vulnerabilities also affects Exchange Server 2010. It is not the first step in the attack chain, but a patch was issued for defense-in-depth purposes. It is still recommended to investigate for potential exploitation.

Feedback & Support

If you have feedback or questions about this issue, please contact us using the ESET Security Forum, or via local ESET Technical Support.

Resources

- Exchange servers under siege from at least 10 APT groups — ESET's WeLiveSecurity blog post
- ESET Research's initial tweets

- Does ESET protect me from the Hafnium zero-day exploit in Microsoft Exchange? — ESET Knowledgebase article
- CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065 — vulnerability details at Microsoft Security Response Center
- HAFNIUM targeting Exchange Servers with 0-day exploits — Microsoft Security blog post
- Multiple Security Updates Released for Exchange Server — Microsoft Security Response Center blog post
- Microsoft Exchange Server Vulnerabilities Mitigations — Microsoft Security Response Center blog post
- March 2021 Exchange Server Security Updates for older Cumulative Updates of Exchange Server — Exchange Team blog post at Microsoft Tech Community