HC3: Alert

September 30, 2022 TLP: White Report: 202209301700

Microsoft Exchange Zero-Day Actively Exploited in Attacks

Executive Summary

Researchers have identified two zero-day vulnerabilities in Microsoft Exchange Server 2013, 2016, and 2019 that are being actively exploited in the wild. Threat actors gain initial access through the following vulnerabilites: CVE-2022-41040, which is a Server-Side Request Forgery (SSRF) vulnerability, and CVE-2022-41082, which allows remote code execution (RCE) when PowerShell is accessible to the attacker. Microsoft Exchange is used in the Healthcare and Public Health (HPH) sector and therefore poses a significant threat.

Report

Customer Guidance for Reported Zero-Day Vulnerabilities in Microsoft Exchange Server
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Impact to HPH Sector

Currently, the full impact to the HPH sector is unknown; however, the threat actors actively exploiting these vulnerabilities make the HPH sector a potential target. According to Microsoft, in a successful attack using CVE-2022-41040, an authenticated threat actor will have the ability to remotely trigger CVE-2022-41082. With this attack, authenticated access to the vulnerable Microsoft Exchange Server is necessary for a threat actor to successfully exploit either of the two vulnerabilities. At this time, there are no patches available, however, Microsoft stated they are aware of the "limited targeted attacks using the two vulnerabilities to get into users' systems" and they are working on an accelerated timeline to release a fix. It is worth noting that Microsoft Exchange Online has detections and mitigations in place to protect customers. Microsoft Exchange Online Customers do not need to take any action. Microsoft Exchange Online has detections and mitigations in place to protect customers. It is recommended that HPH organizations with on-premises Microsoft Exchange review and follow Microsoft's guidance to apply necessary mitigations and patches once they become available.

References

Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Microsoft says two new Exchange zero-day bugs under active attack, but no immediate fix
https://techcrunch.com/2022/09/30/microsoft-exchange-zero-days/

Unpatched Microsoft Exchange Zero-Day actively exploited in the wild
https://securityaffairs.co/wordpress/136433/hacking/microsoft-exchange-zero-day-2.html

Stop us if you've heard this one before: Exchange Server zero-day being actively exploited
https://www.theregister.com/2022/09/30/exchange_server_zero_day/

Zero-Day Exploit in-the-Wild Exchange
Warning: New Attack Campaign Utilized a New 0-Day RCE Vulnerability on Microsoft Exhange Server
https://www.gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-

microsoft-exchange-server-12715.html

SECURITY ALERT: Attack Campaign Utilizing Microsoft Exchange 0-Day (CVE-2022-41040 and CVE-2022-41082)
https://success.trendmicro.com/dcx/s/solution/000291651?language=en_US

Two Microsoft Exchange zero-days exploited by attackers (CVE-2022-41040, CVE-2022-41082)
https://www.helpnetsecurity.com/2022/09/30/cve-2022-41040-cve-2022-41082/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback