Microsoft Identifies New Cyberattack Exploits, Issues Patches for On-Premises Exchange Servers

UPDATED MAR. 3, 2021

March 2, 2021 - Microsoft announced tonight that it has identified new nation-state cyberattacks using previously unknown exploits that target the company's on-premises Exchange Server software. As a result, to minimize or avoid impacts of this situation, **Microsoft highly recommends that you take immediate action to apply the patches for any on-premises Exchange deployments** you have or are managing for a customer or advise your customer of the steps they need to take. The vulnerabilities exist in on-premises Exchange Servers 2010, 2013, 2016, and 2019. Exchange Online is not affected.

Read the Microsoft Blog: New nation-state cyberattacks
Read the Microsoft Exchange Blog: Released - March 2021 Exchange Server Security Updates

The priority are servers which are accessible from the Internet (*e.g.*, servers publishing Outlook on the web/OWA and ECP). To patch these vulnerabilities, you should move to the latest Exchange Cumulative Updates and then install the relevant security updates on each Exchange Server.

- You can use the Exchange Server Health Checker script, which can be downloaded from GitHub (use the latest release).
- Running this script will tell you if you are behind on your on-premises Exchange Server updates (note that the script does not support Exchange Server 2010).
- We also recommend that your security team assess whether or not the vulnerabilities were being exploited by using the Indicators of Compromise we shared here.

Resources and information about this issue for partners

- Microsoft On the Issues blog
- Microsoft Security Response Center (MSRC) release - Multiple Security Updates Released for Exchange Server
- Exchange Team Blog
- MSTIC Blog
- MSRC Blog
- Microsoft On the Issues Blog
- Out of Band Exchange Release Customer Alert
- Security Update Guide

Exchange patch information

- March 2, 2021 Security Update Release - Release Notes - Security Update Guide - Microsoft
- CVE-2021-26855 | Microsoft Exchange Server Remote Code Execution Vulnerability (public)
- CVE-2021-26857 | Microsoft Exchange Server Remote Code Execution Vulnerability (public)
- CVE-2021-26858 | Microsoft Exchange Server Remote Code Execution Vulnerability (public)
- CVE-2021-27065 | Microsoft Exchange Server Remote Code Execution Vulnerability (public)