Remediation Steps for the Microsoft Exchange Server Vulnerabilities

unit42.paloaltonetworks.com/remediation-steps-for-the-Microsoft-Exchange-Server-vulnerabilities

March 9, 2021

By Unit 42

March 9, 2021 at 9:40 AM

Category: Unit 42

Tags: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, Microsoft Exchange Server, vulnerabilities

This post is also available in: 日本語 (Japanese)

Background

On March 2, the security community became aware of four critical zero-day Microsoft Exchange Server vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065).

These vulnerabilities let adversaries access Exchange Servers and potentially gain long-term access to victims' environments. While the Microsoft Threat Intelligence Center (MSTIC) attributes the initial campaign with high confidence to HAFNIUM, a group they assess to be state-sponsored and operating out of China, multiple threat intelligence teams, including MSTIC and Unit 42, are also seeing multiple threat actors now exploiting these zero-day vulnerabilities in the wild. Estimated number of potentially compromised organizations is in the tens of thousands globally – and very importantly, these vulnerabilities were being actively exploited for at least two months before the security patches were available. As a result, even if you patched immediately, your Exchange Servers could still be compromised. Further, based on telemetry collected from the Palo Alto Networks Expanse platform, we estimate there remain over 125,000 unpatched Exchange Servers in the world.

Below you will find a concise playbook that enterprises can follow to respond to this potential threat in their environments.

1) Locate all Exchange Servers and determine whether they need to be patched.

Exchange Online is not affected.

Vulnerable Exchange Server versions include 2013, 2016, and 2019. While Exchange 2010 is not vulnerable to the same attack chain as Exchange 2013/2016/2019, Microsoft has released a patch for CVE-2021-26857 for this version of the software. Microsoft has recently released additional guidance for older, unsupported versions of Exchange.

Microsoft is recommending to install updates on all Exchange Servers, prioritising those that are externally/internet facing. Even if Exchange Servers are not internet facing, the vulnerabilities can still be exploited if access to the network has been achieved through other methods.

Microsoft has published information about the updates for the following specific versions of Exchange Server:

Exchange Server 2019 (update requires Cumulative Update (CU) 8 or CU 7).

Exchange Server 2016 (update requires CU 19 or CU 18).

Exchange Server 2013 (update requires CU 23).

Exchange Server 2010 (update requires SP 3 or any SP 3 RU – this is a Defense in Depth update).

2) Patch and secure all Exchange Servers.

Install the out-of-band security updates for your version of Exchange Server.

If you cannot update and/or patch an Exchange Server immediately, there are some mitigations and workarounds that may reduce the chances of an attacker exploiting an Exchange Server; these mitigations should only be temporary until patching can be completed. Palo Alto Networks Next-Generation Firewalls (NGFWs) updated to Threat Prevention Content Pack 8380 or later protect against these vulnerabilities if SSL decryption is enabled for inbound traffic to the Exchange Server. Cortex XDR running on your Exchange Server will detect and prevent webshell activity commonly used in these attacks.

The initial attack requires the ability to make an untrusted connection to Exchange Server port 443. You can protect against this by restricting access to the system from untrusted users. This can be achieved by only allowing access to the system from users who have already authenticated through a VPN, or by using a firewall to limit access to specific hosts or IP ranges. 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 to the network or can convince an administrator to open a malicious file.

More information about using Palo Alto Networks products, including firewalls with security subscriptions, Cortex XSOAR for automation and Cortex XDR for endpoint protection, can be found in our Threat Assessment.

3) Determine whether an Exchange Server has already been compromised.

These vulnerabilities have been in the wild and actively exploited for over a month, with the earliest indications of exploitation leading back to Jan. 3. Any organization running the vulnerable software must evaluate if their server has been compromised. Patching the system will not remove any malware already deployed on the system. It would be prudent to assume Exchange Servers that exposed Outlook Web Access or Exchange Web Services to the internet are compromised until proven otherwise.

Check for suspicious process and system behavior, especially in the context of Internet Information Service (IIS) and Exchange application processes, such as PowerShell, Command shells (cmd.exe) and other programs executed in the applications' address space. We describe how to use Palo Alto Networks Cortex XDR Pro endpoint protection to hunt for this attack in your environment in "Hunting for the Recent Attacks Targeting Microsoft Exchange."

Microsoft has released PowerShell and Nmap scripts for checking your Exchange Server for indicators of compromise of these exploits. They have also released another script, available at the same link, that highlights differences in files from the virtual directories of your

Exchange Server against those expected for your specific Exchange version. The Cybersecurity and Infrastructure Security Agency (CISA) has also published a list of tactics, techniques and procedures (TTPs).

As documented in the Unit 42 Threat Assessment Courses of Action table, the post-intrusion TTPs used by the initial actors conducting the Exchange attacks included the following:

- Using Procdump to dump the LSASS process memory.
- Using 7-Zip to compress stolen data into ZIP files for exfiltration.
- Adding and using Exchange PowerShell snap-ins to export mailbox data.
- Using the Nishang Invoke-PowerShellTcpOneLine reverse shell.
- Downloading PowerCat from GitHub, then using it to open a connection to a remote server.

Since the initial attacks, we believe that other actors are trying to capitalize on the Exchange vulnerabilities, but their motivations and objectives may differ vastly, and so could their TTPs.

4) Engage an Incident Response team if you think you have been compromised.

If, at any point, you think your Exchange Server has been compromised, you should still take action to secure it against the vulnerabilities as described above. This will prevent additional adversaries from further compromising the system. Installing the out-of-band security updates for your version of Exchange Server is very important, but this will not remove any malware already installed on systems and will not evict any threat actors present in the network.

The potential impact of this situation is critical due to the ongoing activity described, the vulnerabilities exploited to deliver the attack and the adversaries who could be behind compromises. While exploits of these vulnerabilities may not halt business operations, access to sensitive information and systems is certainly possible, and should be assumed to have occurred. Access to corporate emails could also lead to followup phishing attacks.

If you believe you have been compromised, you should enact your incident response plan. If you need such services, our Palo Alto Networks Crypsis incident response team is available to help: crypsis-investigations@paloaltonetworks.com.

Additional Resources:

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.