On-Premises Exchange Server Vulnerabilities Resource Center – updated March 25, 2021

msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server

MSRC / By MSRC Team / March 2, 2021

On March 2nd, we released several security updates for Microsoft Exchange Server to address vulnerabilities that are being used in ongoing attacks. Due to the critical nature of these vulnerabilities, we recommend that customers protect their organizations by applying the patches immediately to affected systems.

The vulnerabilities affect Exchange Server versions 2013, 2016, and 2019, while Exchange Server 2010 is also being updated for defense-in-depth purposes. Exchange Online is not affected.

These vulnerabilities are being exploited as part of an attack chain. The initial attack requires the ability to make an untrusted connection to the Exchange server, but other portions of the attack can be triggered if the attacker already has access or gets access through other means. This means that mitigations such as restricting untrusted connections or setting up a VPN will only protect against the initial portion of the attack to change the attack surface or partially mitigate, and that patching is the only way to mitigate completely.

Since these patches were released, we have published several articles and blog posts helping customers understand these vulnerabilities, and their exploitation patterns, and shared detailed guidance on how the malicious actors are exploiting these vulnerabilities and targeting customers. We are aware that there is a lot of detail to understand and are adding this summary of Microsoft's guidance for security incident responders and Exchange administrators on what steps to take to secure their Exchange environments.

Organizations should review and digest the entirety of this guidance before taking action, as the specific order of actions taken to achieve the response objectives is situational and depends on the outcomes of the investigation.

Executive Summary and Background Information

Microsoft continues to investigate the extent of the recent Exchange Server on-premises attacks. Our goal is to provide the latest threat intelligence, Indicators of Compromise (IOC)s, and guidance across our products and solutions to help the community respond, harden infrastructure, and begin to recover from this unprecedented attack. As new information becomes available, we will make updates to this article at https://aka.ms/ExchangeVulns

- March 25, 2021 – Analyzing attacks taking advantage of the Exchange Server vulnerabilities
- March 25, 2021 – Web Shell Threat Hunting with Azure Sentinel
- March 18, 2021 – Automatic on-premises Exchange Server mitigation now in Microsoft Defender Antivirus
- March 16, 2021 – Guidance for responders: Investigating and remediating on-premises Exchange Server vulnerabilities
- March 15, 2021 –One-Click Microsoft Exchange On-premises Mitigation Tool
- March 8, 2021 – March 8 Exchange Team Blog
- March 5, 2021 – Microsoft Exchange Server Vulnerabilities Mitigations
- March 2, 2021 – Microsoft Security Blog: Hafnium Targeting Exchange
- March 2, 2021 – Microsoft on the Issues
- March 2, 2021 – Exchange Team Blog

Overview of the Attack and Exploitation

Microsoft originally followed the adversary group HAFNIUM launching targeted attacks against specific organizations. Recently other adversary groups have started targeting these vulnerabilities, and we expect that these attacks will continue to increase as attackers investigate and automate exploitation of these vulnerabilities. Not all these footholds are being utilized immediately, and some were likely put in place for future exploitation. A detailed overview is available here: *HAFNIUM targeting Exchange Servers with 0-day exploits – Microsoft Security*

While some adversary groups are installing web shells as broadly as possible for future use, some are also conducting further operations on compromised servers and attempting to move laterally into organizations' environments to establish deeper persistence. This document provides instructions to remediate web shells and determine the initial ingress of an adversary.

Organizations that have detected or suspect more advanced post exploitation activities, such as credential dumps, lateral movement, and installation of further malware/ransomware, should consider enlisting the services of cybersecurity response professionals. Investigating and remediating post-exploitation across an IT environment is beyond the scope of this blog, but we want organizations to understand where we recommend they begin their investigations based on the patterns of behavior we've seen associated with exploitation of these vulnerabilities.

Recommended Response Steps

Successful response requires being able to communicate without the attacker eavesdropping on your communications. Until you have achieved assurance of the privacy of your communications on your current infrastructure, use completely isolated identities and

communication resources to coordinate your response and discuss topics that could potentially tip off the attacker to your investigation.

Successful response should consist of the following steps:

1. Deploy updates to affected Exchange Servers.

1. Investigate for exploitation or indicators of persistence.

1. Remediate any identified exploitation or persistence and investigate your environment for indicators of lateral movement or further compromise.

Microsoft recommends that you update and investigate in parallel, but if you must prioritize one, prioritize updating and mitigation of the vulnerability.

It is imperative that you update or mitigate your affected Exchange deployments immediately. These vulnerabilities are being actively exploited by multiple adversary groups. For the highest assurance, block access to vulnerable Exchange servers from untrusted networks until your Exchange servers are patched or mitigated. If you have not yet patched, and have not applied the mitigations referenced below, a one-click tool, the Exchange On-premises Mitigation Tool is now our recommended path to mitigate until you can patch.

If you are an experienced IT professional or incident responder, review our Guidance for Responders post for more detailed recommendations that will be continually updated when Microsoft has new information about responding to these attacks.

Deploy updates to affected Exchange Servers

If you do not have an inventory of servers in your environments that run Exchange, you can use the nmap script Microsoft has provided to scan your networks for vulnerable Exchange deployments. For the Exchange servers in your environment, immediately apply updates for the version of Exchange you are running. While these Security Updates do not apply to Exchange Online / Office 365, if you are in Hybrid mode you need to apply them to your on-premises Exchange Server, even if it is used for management purposes only. You do not need to re-run (Hybrid Configuration Wizard) HCW if you are using it. The high-level summary of our patching guidance is:

- **Exchange Online is not affected.**
- **Exchange 2003 and 2007** are no longer supported but are not believed to be affected by the March 2021 vulnerabilities. You must upgrade to a supported version of Exchange to ensure that you are able to secure your deployment against vulnerabilities fixed in current versions of Microsoft Exchange and future fixes for security issues.
- **Exchange 2010** is only impacted by CVE-2021-26857, which is not the first step in the attack chain. Organizations should apply the update and then follow the guidance below to investigate for potential exploitation and persistence.

Exchange 2013, 2016, and 2019 are impacted. Immediately deploy the updates or apply mitigations described below. For help identifying which updates you need to get from your current CU version to a version with the latest security patches follow this guidance: Released: March 2021 Exchange Server Security Updates – Microsoft Tech Community. You can use the linked Health Checker script here to help you identify exactly which CUs are needed for your deployment. Microsoft has also released additional Security Updates for select older Exchange CUs to accelerate their path to patched for these vulnerabilities.

Mitigations: If for some reason you cannot update your Exchange servers immediately, we have released instructions for how to mitigate these vulnerabilities through reconfiguration. We recognize that applying the latest patches to Exchange servers may take time and planning, especially if organizations are not on recent versions and/or associated cumulative and security patches. We recommend prioritizing installing the patches on Exchange Servers that are externally facing first, but all affected Exchange Servers should be updated urgently. The Mitigations suggested **are not substitutes for installing the updates** and will impact some Exchange functionality while in place. Detailed guidance on applying the alternate mitigations is provided here:*Microsoft Exchange Server Vulnerabilities Mitigations – March 2021*.

Applying the update or the alternative mitigation techniques will not evict an adversary who has already compromised your environment. The remainder of this document shares guidance to help you determine whether your Exchange servers were exploited before mitigating the issue and how to remediate some types of attacks.

Investigate for exploitation, persistence, or evidence of lateral movement

In addition to protecting your Exchange servers from exploitation, you should assess to ensure that the vulnerabilities were not exploited *before* you got them to a protected state.

1. **Analyze the Exchange product logs for evidence of exploitation**. Microsoft released detailed steps here including scripts to help automate: *Scan Exchange log files for indicators of compromise*. If you choose to use the script provided, you will have an option to scan some or all of your Exchange servers at the same time.

1. **Scan for known web shells.** The Microsoft Defender team has included security intelligence for known malware related to these vulnerabilities in the latest version of the Microsoft Safety Scanner. Run this Safety Scanner on every Exchange server in your environment. If you need assistance, detailed guidance can be found here: CSS-Exchange/Defender-MSERT-Guidance.md at main · microsoft/CSS-Exchange · GitHub

For Microsoft Defender and Microsoft Defender for Endpoint customers, please make sure you are on the latest security intelligence patch: *Latest security intelligence patches for*

Microsoft Defender Antivirus and other Microsoft antimalware – Microsoft Security Intelligence

1. **Use the Microsoft IOC feed for newly observed indicators.** To aid defenders in investigating these attacks where Microsoft security products and tooling may not be deployed, we are releasing a feed of observed indicators of compromise (IOCs). The feed of malware hashes and known malicious file paths observed in related attacks is available in both JSON and CSV formats at the below GitHub links. This information is being shared as TLP:WHITE (free for all to use)

- **CSV format**
- **JSON format**

1. **Leverage other organizational security capabilities** in addition to these tools. The tools above make the threat intelligence that Microsoft has been accumulating related to exploitation of these vulnerabilities available to all organizations. Your organization may also have its own security controls, and we recommend that you increase your vigilance on signals from Exchange servers in your current security controls too.

Remediate any identified exploitation or persistence

If you find any evidence of exploitation (e.g., in Exchange application logs), ensure you are retaining the logs, and use the details such as timestamps and source IPs to drive further investigation.

If you find known bad files using your endpoint security solution, the Microsoft IOC feed, or the Microsoft Safety Scanner, take the following actions:

1. Remediate and quarantine them for further investigation unless they are expected customizations in your environment.

1. Search your IIS logs to identify whether or not the files identified as malicious have been accessed.

1. Consider submitting suspected malicious files to Microsoft for analysis following this guidance: Submit files for analysis by Microsoft – Windows security | Microsoft Docs and include the string “ExchangeMarchCVE” in the Additional Information text box of the submission form.

As part of hunting and scanning, if you find evidence of exploitation of the Unified Messaging RCE (CVE-2021-26857), you should delete potential uncleaned exploit files in %ExchangeInstallPath%\UnifiedMessaging\voicemail

If you find any evidence of external access to a suspect file identified above, use this information to drive further investigation on impacted servers and across your environment. Our blog post on the Hafnium attack goes into details for folks who need additional details for IOC's, File Hashes, etc.: HAFNIUM targeting Exchange Servers with 0-day exploits – Microsoft Security

If any of your security detections or the investigation tools results lead you to suspect that your Exchange servers have been compromised and an attacker has actively engaged in your environment, execute your Security Incident Response plans, and consider engaging experienced Incident Response assistance. It is particularly critical if you suspect that your Exchange environment is compromised by a persistent adversary that you coordinate your response using alternative communications channels as mentioned earlier in this document.