2021

HAFNIUM Exchange Server Exploits

Server Critical Update Guide:

STEPHEN STRETZ

HAFNIUM EXCHANGE SERVER EXPLOITS

SERVER CRITICAL UPDATE GUIDE

PURPOSE

The purpose of this document is to educate partners on the best method for protecting their current Exchange On-prem servers from the most recent HAFNIUM 0-day exploit(s).

AUDIENCE

All Pax8 Partners

LAST UPDATED

March 2021

Step-by-Step Guide

This Server Critical Update Guide consists of 4 Major Steps:

Step 1: HAFNIUM 0-day vulnerability

As of March 2nd, 2021, multiple exploits related to Exchange servers running Exchange 2013, 2016, and 2019 has been identified by Microsoft Threat Intelligence Center (MSTIC) and has been attributed to a group known as HAFNIUM.

These exploits potentially enable hackers to access email accounts and install malware for long-term access to victim environments. This document is designed to assist Pax8's partners in alerting their clientele of the danger and setting plans in motion to identify the risk and resolve it.

The specific vulnerabilities to be addressed are identified as: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.

For more information on Microsoft's official post related to these attacks, please see the below link: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

While Microsoft will be addressing these vulnerabilities within their new CU updates to various Exchange systems within the March 2021 timeframe, it is highly recommended to install the recently released Service Updates to combat these vulnerabilities as soon as possible.

Step 2: Has my server been compromised already?

One's first reaction to this news may be, "Is my system already compromised?". In order to best determine the indicators of compromise (IOCs), Microsoft put together a list of ways to search for these possible intrusions. The below information was taken directly from this article:

Scan Exchange log files for indicators of compromise

- CVE-2021-26855 exploitation can be detected via the following Exchange HttpProxy logs:
  - These logs are located in the following directory: %PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\HttpProxy
  - Exploitation can be identified by searching for log entries where the AuthenticatedUser is empty and the AnchorMailbox contains the pattern of ServerInfo~*/*
    - Here is an example PowerShell command to find these log entries:

Import-Csv -Path (Get-ChildItem -Recurse -Path "$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -Filter '.log').FullName | Where-Object { $_.AuthenticatedUser -eq '' -and $_.AnchorMailbox -like 'ServerInfo~*/*' } | select DateTime, AnchorMailbox*

  - If activity is detected, the logs specific to the application specified in the AnchorMailbox path can be used to help determine what actions were taken.
    - These logs are located in the %PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging directory.
- CVE-2021-26858 exploitation can be detected via the Exchange log files:
  - C:\Program Files\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog
  - Files should only be downloaded to the %PROGRAMFILES%\Microsoft\Exchange Server\V15\ClientAccess\OAB\Temp directory
    - In case of exploitation, files are downloaded to other directories (UNC or local paths)
  - Windows command to search for potential exploitation:
  -

findstr /snip /c:"Download failed and temporary file" "%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog.log"*

- CVE-2021-26857 exploitation can be detected via the Windows Application event logs
  - Exploitation of this deserialization bug will create Application events with the following properties:
    - Source: MSExchange Unified Messaging
    - EntryType: Error
    - Event Message Contains: System.InvalidCastException

Step 2: Has my server been compromised already? (Continued)

- Following is PowerShell command to query the Application Event Log for these log entries:

*Get-EventLog -LogName Application -Source "MSExchange Unified Messaging" -EntryType Error | Where-Object { $_.Message -like "*System.InvalidCastException*" }*

- CVE-2021-27065 exploitation can be detected via the following Exchange log files:
  - C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Server

All Set-<AppName>VirtualDirectory properties should never contain script. InternalUrl and ExternalUrl should only be valid Uris.

- Following is a PowerShell command to search for potential exploitation:

Select-String -Path "$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\ECP\Server.log" -Pattern 'Set-.+VirtualDirectory'*

Step 3: Identify and Prepare Exchange environment

Microsoft has released a set of new updates for Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019 to address these concerns. It is highly encouraged both from Microsoft and from Pax8 that these servers be patched as soon as possible to ensure the safety and security of all systems that could be potentially affected. Please be aware that these security updates can only be installed on an Exchange Server that already at a specific minimum patch level. Please see below:

- Exchange Server 2010 SP3 14.3.123.4
- Exchange Server 2013 CU23 15.0.1497.2
- Exchange Server 2016 CU18+ 15.1.2106.2
- Exchange Server 2019 CU7+ 15.2.721.2

To validate your current version of Exchange, please open the Exchange Management Shell on your server and run the below cmdlets based on which version of Exchange you have:

- **Exchange Server 2010**
    - Get-Command ExSetup | ForEach {$_.FileVersionInfo}

- **Exchange Server 2013, 2016, 2019**
    - Get-ExchangeServer | Format-List Name,Edition,AdminDisplayVersion

You can compare the output from these commands against the versions listed here to verify if you have the correct patch level required.

Step 3: Identify and Prepare Exchange environment (Continued)

If your version of Exchange does not meet the minimum requirements as documented above, you will first need to run updates to your Exchange server to meet these requirements. These updates will require server downtime and reboots. It is highly recommended to plan for these outages and create new backups of your servers prior to installing them. Please ensure that every precaution is taken prior to running these updates on live environments. You will find the most recent CU download link below for each version of Exchange:

- **Exchange 2010**
  - Service Pack 3 : Info Download Link
- **Exchange 2013**
  - Cumulative Update 23 : Info Download Link
- **Exchange 2016**
  - Cumulative Update 19 : Info Download Link
- **Exchange 2019**
  - Cumulative Update 8 : Info Download Link

Make sure to download the package(s) to the server to-be-updated and run the executable installers as an administrator. As mentioned before, ensure you have a planned downtime with your client's / end-users and proper backups have been taken prior to installing any new updates. As with all installations, ensure that all other software is closed, antivirus is temporarily turned off, and no other potential conflicts are present when running the installation. After the installation is finished, ensure that the server is rebooted to finalize the installation of the update, the server comes back online successfully, and the Exchange services all are running. Perform any required testing to ensure Exchange mail-related functionality post-reboot as required before continuing to install the service update.

After you have completed the update, re-run the aforementioned cmdlets to ensure the build number is correctly up-to-date:

- **Exchange Server 2010**
  - Get-Command ExSetup | ForEach {$_.FileVersionInfo}

- **Exchange Server 2013, 2016, 2019**
  - Get-ExchangeServer | Format-List Name,Edition,AdminDisplayVersion

Step 4: Download and Install Service Update

Please ensure that prior to going through this section that you have read through the previous stages the ensure the current Exchange environment can support the new service updates. If the Exchange server does meet the minimum requirements expressed previously, then proceed as below.

As mentioned before, Microsoft has released Security Updates to combat the aforementioned vulnerabilities within Exchange environments. Their response and information can be found here. These updates come to us in the form of the KB50000871 for Exchange Server 2013 through 2019 and KB50000978 for Exchange Server 2010. To obtain these updates, you can find them in 3 different methodologies.

Method 1: Microsoft Update
This update is available from Microsoft Update. When you turn on automatic updating, this update will be downloaded and installed automatically. For more information about how to get security updates automatically, see Windows Update: FAQ.

Method 2: Microsoft Update Catalog
To get the standalone package for this update, go to the Microsoft Update Catalog website.

Method 3: Microsoft Download Center
You can get the standalone update package through the Microsoft Download Center. You can find the downloads below:

- **Exchange Server 2010** : Info Download Link
- **Exchange Server 2013** : Info Download Link
- **Exchange Server 2016** : Info
  - Cumulative Update 18 : Download Link
  - Cumulative Update 19 : Download Link
- **Exchange Server 2019** : Info
  - Cumulative Update 7 : Download Link
  - Cumulative Update 8 : Download Link

If you opted to download the Service Update packages directly, make sure to download the package(s) to the server to-be-updated and run the executable installers as an administrator. As mentioned before, ensure you have a planned downtime with your client's / end-users and proper backups have been taken prior to installing any new updates. As with all installations, ensure that all other software is closed, antivirus is temporarily turned off, and no other potential conflicts are present when running the installation. After the installation is finished, ensure that the server is rebooted to finalize the installation of the update, the server comes back online successfully, and the Exchange services all are running. Perform any required testing to ensure Exchange mail-related functionality post-reboot as required.

Resource: Check the Patch Health of your Exchange Server

Microsoft has provided an excellent resource for validating Exchange Server Health called HealthChecker.ps1. You can get it on GitHub, along with usage instructions here.

Additional: Contact Support

If you have any questions or concerns related to these exploits, vulnerabilities, update methods, or this document please do not hesitate to reach out to your Pax8 representative for more information. For additional assistance, please reach out to your CSA or our support team:

Support (Existing Partners Only)
- Support: 1-855-884-7298 Ext. 3
- Email: support@pax8.com
- Hours: 24/7

I hope this article provided the appropriate assistance in ensuring that your client's Exchange environments remain secure after the identification of the recent vulnerabilities noted in this document. Any feedback to improve this guide further would be greatly appreciated and can be sent to the following email:

feedback@pax8.com