HAFNIUM – SELF-HELP GUIDE

First Steps To Mitigating the Security Vulnerabilities In Microsoft Exchange Server

Status: Version 1.6, 24.03.2021, 01:00

STATUS & FACTS

On March 3rd, 2021, Microsoft released so-called out-of-band (i.e., urgent and critical) updates for its Exchange Server product. Installing these patches right away is absolutely necessary due to the four “HAFNIUM” vulnerabilities already being used by attackers to access confidential data or install malware.

Note: In this document, currently available information is used to define a possible course of action. The document will be updated on an ongoing basis. Therefore, please check back regularly at

https://research.hisolutions.com/

AFFECTED SYSTEMS

According to the vendor,[1] the following systems are affected:

- Exchange 2010 (only CVE-2021-26857)
- Exchange 2013
- Exchange 2016
- Exchange 2019

Exchange 2003 or 2007 are probably not affected. However, support for these systems has been discontinued and they have other critical vulnerabilities and should therefore be updated to a current version immediately!

The cloud service Exchange Online is NOT affected.

[1] https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

TLP:WHITE

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

+49 30 533 289-0
+49 30 533 289-900

STEPS TO MITIGATE THE VULNERABILITIY

Step 1: Preventing further attacks

Note: The following steps contain measures that should be carried out by technically experienced personnel. If in doubt, please give this document to your IT service provider, who can work through these steps with you.

Since the vulnerabilities are being exploited actively, we recommend the following steps to prevent acute infection before searching for possible compromises:

- If not already done: Immediately install the security updates released by Microsoft, where immediately means within the next 2 hours after receiving this information.
    - If it is not possible to update using the security update provided by Microsoft, the following measures recommended by Microsoft[2] should be carried out:
        - Disable Unified Messaging (UM)
        - Disable Exchange Control Panel (ECP) VDir
        - Disable Offline Address Book (OAB) VDir
        - Disable Active Sync
        - Disable Outlook Web Access (OWA)
- Additionally it is recommended to immediately block port 443 on the firewall or disconnect the Exchange server from the Internet until the patches are applied. (If this measure is possible and does not delay the installation of the security updates)

NOTE: We also urgently advise you to check if there is the need to report a PII data breach under the GDPR or national Data Protection Act.

Step 2: Verifying a possible compromise

To check your systems for a possible compromise:

1. Save the following data for possible later analysis, e.g. by saving a full backup or snapshot (incl. memory) of the Exchange system.
    - Exchange Server
        - IIS-Server log files extracted from C:\inetpub\Logs\
        - Exchange Server log files extracted from <Exchange_Installation_Path>\v15\Logging\ (at least from the 24.02.)
        - Content of the inetpub folder
        - All Windows Event Logs (C:\Windows\System32\winevt\logs\)
    - Domain Controller
        - all Windows Event Logs (C:\Windows\System32\winevt\logs\)
2. Perform an offline backup (e.g., to an external hard disk) of system backups (Exchange and domain from the last backup state before 03/02/2021).

[2] https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

3. Run the Microsoft test scripts[3] (Test-ProxyLogon.ps1 and CompareExchangeHashes.ps1). Please follow their instructions carefully.

   As a result, you will receive a CSV file that you can analyze:

	H	I
	AnchorMailbox	HttpStatus
	ServerInfo~a]@contoso.com:444/autodiscover/autodiscover.xml?#	200
	ServerInfo~a]@contoso.com:444/autodiscover/autodiscover.xml?#	200
	ServerInfo~akak]@contoso.com:444/autodiscover/autodiscover.xml?#	200
	ServerInfo~akak]@contoso.com:444/mapi/emsmdb/?#	200
	ServerInfo~akak]@contoso.com:444/ecp/proxyLogon.ecp?#	241
N1	ServerInfo~a]@contoso.com:444/autodiscover/autodiscover.xml?#	200
	ServerInfo~a]@contoso.com:444/mapi/emsmdb/?#	200
	ServerInfo~a]@contoso.com:444/ecp/proxyLogon.ecp?#	241

Figure 1: Example output of the Microsoft test script[3]

NOTE: For organizations lacking an incident response service provider, Microsoft have released an automated tool for checking affected systems.[4] The tool implements emergency measures and attempts to reverse changes made to the systems by attackers. At present, we have no empirical values on the reliability of the new tool.

Option 1: Probably NO compromise
If you see no entries or only entries ending in

```
444/autodiscover/autodiscover.xml?#","200"
```

we and Microsoft[5] currently assume that there was no successful compromise. The entry is an indication that one of the mentioned vulnerabilities was being exploited but the attacker did not find a valid email address. You should still follow the "preventive measures" below.

Option 2: Probably a compromise
If you see other entries like

```
444/mapi/emsmdb/?#","200"
444/ecp/proxyLogon.ecp?#","241"
```

we assume compromise of your system. If this is the case you should start implementing the measures listed under “Step 3: Recommended measures (when possibly compromised)” immediately.

NOTE: A vulnerability was used to access your Exchange Server IT system. Thus, an attacker was able to access personal data on your IT system. Whether the attackers actually used this possibility has not been confirmed at this point.

[3] https://github.com/microsoft/CSS-Exchange/tree/main/Security
[4] https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/
[5] https://github.com/microsoft/CSS-Exchange/commit/19778cd80c98b5c395079ef9d1f3ac1d1b059a40

Therefore, please check with your data protection officer whether a report under the GDPR should be submitted within 72h.

4. Use the Thor-Lite scanner[6]. A manual (in German) has been published in our research blog.[7]

REMARK: In older versions of this document we recommended the use of the Microsoft Support Emergency Response Tool (MSERT). Although this tool is helpful, we advise caution when using it. MSERT may delete shells and may not ensure complete cleanup. We recommend using it with the /N option and backing up the files it finds. Thus, the data is not deleted and can still be examined by a specialist afterwards.

Step 3: Recommended measures (when possibly compromised)

So far, the attackers' goals and motives for attacking the Exchange server are still unknown. The number of attacker groups has increased significantly since the release of the out-of-band patches and the following publications. For this reason, it is currently impossible to say which measures are sufficient to fully restore the compromised systems.

In typical attacks, attackers automatically access your address books and emails. As a first step, you should check for further successful attacks by checking for the existence of so-called "web shells".

The vulnerability is already being exploited by several groups, so searching for web shells of the originating group is not sufficient. The BSI (the German Federal Office for Information Security) has published an overview in the document "Microsoft Exchange Vulnerability Detection and Response"[8] about possible ways to search for web shells.

Please check the following directories including subdirectories for .aspx files that were either recently changed or created (during the last month) or which are owned by the user „NT AUTHORITY\SYSTEM“.

- C:\inetpub\wwwroot\aspnet_client\
- <Exchange installation path>\V15\FrontEnd\HttpProxy\owa\auth\
- C:\Exchange\FrontEnd\HttpProxy\owa\auth\

NOTE: The paths given are sample paths. The exact paths may differ depending on the installation location and Exchange version.

Additionally, you can use the Thor-Lite scanner[6] to detect possible web shells. We published a German manual in our research blog. (The detection script created by the Latvian CERT[9] we previously recommended is no longer updated.)

[6] https://www.nextron-systems.com/thor-lite/
[7] https://research.hisolutions.com/
[8] https://bsi.bund.de/exchange-schwachstellen
[9] https://github.com/cert-lv/exchange_webshell_detection

There is an extensive list[10] stating possible names of web shells.

NOTE: Due to the number of possible attackers, this can only be seen as an indication. Please regularly check your systems with current and updated signatures.

NOTE: Your presumed date of compromise is currently counted as the first occurrence of a web shell on your systems. If HiSolutions incident managers are supporting you, they can help you with the assessment.

Option 1: No web shell was found

Raise your staff's, partners', customers' and service providers' awareness concerning possible phishing attacks including current insider information and processes.

Perform a full anti-virus scan of your IT (e.g. using Microsoft Security Scanner MSERT[11]).

NOTE: In older versions of this document, we recommended the use of the Microsoft Support Emergency Response Tool (MSERT)[12]. Although this tool is useful, we currently recommend caution when using MSERT. It may delete shells and may not ensure complete cleanup. We recommend using it with the /N option and backing up the files it finds. In this case, the data is not deleted and can still be examined by a specialist afterwards. During the scan, files may be displayed as infected. However, these are only marked as "suspicious" in the first step and are analyzed again in the Microsoft cloud given Internet access. If the result is negative, the mark is removed. When in doubt, MSERT shows no findings as the final result, even though there were findings present during the scan.

Restoring a backup of the compromised Exchange Server is recommended. (Backup dated before 03/02/2021 or before your identified date of compromise).

Make sure you completed the following steps:

- Install all patches made available by Microsoft.
- Thoroughly change all usernames and passwords, especially of administrative accounts.
- Reset the domain controller password/computer account for Exchange Server.[13]
- Implement the measures listed under "Preventive Measures".

Option 2: A web shell was found

This can be an indication of further compromise. According to BSI recommendations[14], your organization should switch to incident response mode.

[10] https://gist.github.com/JohnHammond/0b4a45cad4f4ed3324939d72dc599883
[11] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
[12] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
[13] https://docs.microsoft.com/de-de/troubleshoot/windows-server/windows-security/use-netdom-reset-domain-controller-password
[14] https://bsi.bund.de/exchange-schwachstellen

Restore your Exchange server from a backup from before 03/02/2021 or your identified date of compromise. The system must be disconnected from the Internet while doing that. Access to the domain is legitimate, if necessary.

Narrowing down the attack is currently not possible. Therefore, you have the following options:

- **Moving your exchange to the cloud**: With this method, the email database can be migrated into the cloud. Azure AD and Exchange Online are operated by Microsoft. This migration should be well-planned and involves risks (changes for users working from home, short-term failure of IT infrastructure). Additionally, it cannot be guaranteed that the attackers are banned from the system.
- **Using a specialized service provider:** If you manage Exchange server yourself, you should check whether outsourcing to a specialized service provider makes sense. This service provider will take care of maintenance and care aspects and should also oversee the protection of the system.
- **Active Directory domain compromise**: If your Active Directory is assumed to be compromised, there are only two options: a completely new setup of the AD or a rescue attempt using Golden Ticket mitigation, renewal of all credentials (incl. service accounts) and verification of all accounts, groups and rights in your AD. We recommend finding an incident response service provider to support this rescue attempt since this is a complex process.
- **Reinstalling or restoring Exchange (Disaster Recovery)**:
    - Export the mailboxes and decommission the legacy system
    - Restore the Exchange server: If you have a non-compromised backup (dated before 03/02/2021 or your date of compromise) you can use this as a restoration point, alternatively you can reinstall a new Exchange server.
    - Be careful not to bring the Exchange server online (accessible from the outside) until you have performed the actions below. The server may be connected to the Internet after all patches have been installed.
    - Microsoft provides a manual for recovery through reinstallation[15].
    - If you plan on restoring your Exchange server from a backup you must make sure your backup is from before the attack. Please also check the backup with the Microsoft test script. Check if there is an updated script available.
    - Restore the backed up mailboxes and reintegrate them.
- **Investigation of your IT environment**: An incident response provider could check your IT environment for hidden attackers. Such an investigation can last weeks. Usually, in case of compromise a complete reinstallation of the environment is recommended.

The following measures in your Windows domain should also be taken as a precaution:

- Changing all administrative passwords
- Resetting the domain controller password/computer account for your Exchange server[13]

[15] https://docs.microsoft.com/en-us/exchange/high-availability/disaster-recovery/recover-exchange-servers?view=exchserver-2019

- Mitigating golden ticket attacks by changing the password of the KRBTGT-account twice[16] [17]
- Checking for recently created user accounts in the Active Directory during the time of compromise focussing on administrative accounts.
- Check the following groups in your Active Directory for newly created or recently changed accounts:
    - "Exchange Organization Administrators"
    - "Exchange Windows Permissions"

[16] https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf
[17] http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf

Preventive Measures

When compromised, we recommend taking the following steps and implementing the measures to prevent, discover and mitigate follow-up attacks:

- Increase of logging activity
  - Increase the minimum retention period of your log files on the following IT systems and make sure there is sufficient storage space:
    - Security log of the domain controller(s)
    - Exchange access logs
    - Web proxy log
    - Firewall logs
  - Detection of relevant events in the log files
    - We recommend using SIGMA rules[18] to automatically monitor your log files
    - Monitor externally reachable remote access points lacking multi-factor authentication (MFA)
- Check your servers with the Microsoft Safety Scanners[19] weekly.
- Use the Thor-Lite[6] scanner. A German manual is published in our research blog.
- Thoroughly change user accounts and passwords, especially privileged accounts.
- Check the Exchange servers for recently created user accounts, services or additional programs, processes or files.
- Manually start a regular full anti-virus scan of your IT systems.
- Consider implementing multi-factor authentication for remote access.
- If not already in place, start performing offline data backups.
- Raise your staff's, partners', customers' and service providers' awareness concerning possible phishing or CEO Fraud attacks including current insider information and processes. Pay special attention to emails referring to previous conversations and changed banking information or delivery addresses. In addition, attackers might want to trick you into opening malicious attachments.

We recommend monitoring your systems according to these recommendations for the next 12 months. In the past, we often have observed 'quiet times' (after the initial compromise up to the actual attack) of around 2-4 months. In some cases, this period even lasted up to 9 months.

Please check the following sites for updated information on Hafnium:

- https://research.hisolutions.com/hafnium
- https://bsi.bund.de/exchange-schwachstellen

[18] https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin
[19] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download