MS-ISAC®
Multi-State Information Sharing & Analysis Center®

MS-ISAC Microsoft Exchange Playbook

Notes from CIRT 3/16/2021:

Please note the following if you have already completed a rebuild of your exchange server and updated it with the most recent patches:

- **As with all zero-day exploits, initial knowledge can be and is significantly limited and fluid as information develops**
- **Based on current industry knowledge of this exploit, a rebuild and updated patching are the best-known actions to take at this time.**
- **Current knowledge of IOCS related to lateral movement or post compromise activity is limited, however, MS-ISAC has established a webpage dedicated to addressing the Microsoft Zero Day Exploit. The webpage will continue to be updated with the most recent information concerning the exploit. The webpage is https://www.cisecurity.org/ms-exchange-zero-day/**
- **CIRT will conduct an initial IR call with you, the case status will initially be set as inactive due to lack of additional information, however, the case can be reactivated as new information develops**
- **This will enable CIRT to focus additional assistance on members who may not possess the same resources to conduct rebuilds and patching of their Exchange environment**
- **Data regarding the incident can still be provided to CIRT and preserved. It is recommended members preserve, if possible, exploit data as well**
- **There has been a significant influx of cases in CIRT related to this exploit. Our desire is to assist as many members as possible. We ask that you please continue to be patient as we triage and work through these cases. We sincerely appreciate the understanding, which many of you have already expressed. Thank you.**
- **Please do not hesitate to ask additional follow up questions or reach out for help**

To assist as many organizations as possible, we have put together the step-by-step information below that can help to investigate any potential impact of this activity.

1 Investigate for signs of initial compromise:

A Run the Microsoft script “Test-ProxyLogon.ps1” from the below link. This tool checks for exploitation attempts against the recent Exchange 0days.

- Reference https://github.com/microsoft/CSS-Exchange/tree/main/Security

B Search the following directories for unexpected “.aspx” files, as well as search within subdirectories. Common webshell names are provided in the Microsoft advisory. Should you find any webshells, please save a copy for our analysis prior to removal.

- Reference: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- %IIS installation path%\aspnet_client\
- %IIS installation path%\aspnet_client\system_web\
- %Exchange Server installation path%\FrontEnd\HttpProxy\owa\auth\
- %Exchange Server Installation%\FrontEnd\HttpProxy\ecp\auth

C Utilize Microsoft's new Exchange On-premises Mitigation Tool (EOMT) to scan for threats on the local exchange system (this will also attempt to clean any identified malware or webshells).

- https://github.com/microsoft/CSS-Exchange/tree/main/Security

If no evidence of compromise is detected in Step 1 or the EOMT script is successful in mitigating identified threats, the system(s) should be fully updated in accordance with Microsoft's guidance and can then be re-introduced into the environment.

If you would like to engage the MS-ISAC CIRT for IR assistance, contact the MS-ISAC SOC with the request, then continue on to complete steps 3 and 4. Our CIRT will be in touch to inform you how to submit the results of your investigation from these steps. If you do not require CIRT assistance, we recommend taking a forensic image to aid in your investigation before moving on to step 4.

2 Isolate the system for investigation

A It is suggested that the system be disconnected from the network (but not shutoff) until an investigation determines the scope of the compromise.

B If you are unable to completely take the system off the network, at a minimum, disable public access to it over port HTTP/S. The initial exploitation and subsequent webshell access are done via this access.

3 Gathering Data

Please try to provide all the following items for CIRT to be able to assist you with the best service. A share link will be provided shortly following this email.

A Utilize KAPE to gather forensics artifacts from the system.

- Download: https://cisecurity.sharefile.com/d-s290ea9e96a5b40fca7a430a6787d7a4f
- Simply download all the files in the above link, put them on the Exchange server/s of interest, and execute “kape.exe”. This should create a .zip file of artifacts for us to analyze within the directory KAPE was executed.

B Provide web server/IIS logs for OWA. Typically located at “C:\inetpub\logs\LogFiles\”, the last three months of logs should suffice.

C Provide any network logs you may have from the time of the incident.

D Provide any AV/EDR/IDS alerts you may have that are related to the incident.

E Run the Microsoft script “Test-ProxyLogon.ps1” from the below link. Upload any subsequent output from the tool.

- https://github.com/microsoft/CSS-Exchange/blob/main/Security/Test-ProxyLogon.ps1

F Provide a copy of any web shells or other suspicious artifacts that you have identified.

G If possible, collect a memory capture and full disk image of the affected system using FTK Imager. Keep these stored somewhere that they can be uploaded should they be required for analysis. *Please do not upload these two items to the MS-ISAC CIRT unless instructed to do so.*

- https://accessdata.com/product-download/

4 Investigation of Post-Compromise:

A Check to see if “Administrator” has been removed from the “Exchange Organization administrators” group. (if applicable)

B Check for unexpected, recently created local users and/or domain users.

C Check for suspicious, recently created .zip, .rar, and .7z files within the “C:\ProgramData\” directory. It is suspected that malicious third parties have been storing compressed data here for data exfiltration.

D Look for suspicious, recently created files within the “C:\windows\temp\” and “C:\root\” directory. Especially suspicious would be any file with a .dmp extension, or have "lsass" in the name. It is suspected that malicious third parties have been storing LSASS dumps here.

E Monitor for unexpected activity on the network, such as:

- Unexpected user logins to systems or logins at strange times.
- AV/EDR/IDS within the environment that could indicate a compromise.
- Strange network activity, such as an influx in outbound traffic or unusual connections to/from the exchange system over non-SMTP ports that could indicate a reverse shell.
- Installed admin applications such as ProcDump or PSExec on systems that should not have them.

F Review local PowerShell event logs for suspicious command execution.

G Conduct enterprise-wide AV scans looking for suspicious activity.

H It is strongly recommended that agencies prepare to restore the Exchange system from backup, if possible. Please do not restore the system from backup unless a full image capture has been taken or our analysis has been completed.

I Additional updated Microsoft Guidance as of 3/9:

- https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/MSTICIoCs-ExchangeServerVulnerabilitiesDisclosedMarch2021.csv

J MS-ISAC page – Exchange Zero Day Vulnerability Response

- https://www.cisecurity.org/ms-exchange-zero-day/

MS-ISAC Microsoft Exchange Playbook WorkFlow