Threat Advisory Report:

HAFNIUM/Exchange Zero-Days

Published: 3/3/2021
Updated: 3/4/2021

Contents

Summary

On March 2nd, 2021, Microsoft Security Response Center released updates related to vulnerabilities affecting on-premises deployments of **Microsoft Exchange Server 2013/2016/2019**. Microsoft also revealed details around active exploitation of these vulnerabilities using zero-day exploits. The exploited vulnerabilities span several classifications, including server-side request forgery (SSRF), deserialization, and a set of arbitrary file write vulnerabilities; all effecting on-premises Exchange deployments. Each of these vulnerabilities had an assigned CVSS base score of 7.8 or higher, placing their severity ratings within the High and Critical range.

In their exposure of the active exploitation of these vulnerabilities, Microsoft provided attribution details for the activity. Per their research, the activity is associated with a state-sponsored group backed by China: **HAFNIUM**. This threat group is actively targeting various industries within the United States, ranging from law firms to defense contractors. This threat group has historically been associated with exploitation of vulnerabilities in publicly accessible services, and specific targeting of Office 365 environments. HAFNIUM also uses readily available open-source tools for their attacks, including **Covenant**, **Nishang**, **PowerCat**, and other common offensive security tools.

We are engaging all relevant teams within the organization to research the threats posed by this adversary, understand how our **GreyMatter Detect**, **Intel**, and **Hunt** capabilities can be applied to identify these threats, and proactively engage our customers to understand the risk that this campaign poses to them.

Threat Details

The HAFNIUM threat group uses a set of zero-day exploits to gain unauthorized access to Exchange user mailboxes and perform remote code execution on the target Exchange Server. These exploits and their corresponding vulnerabilities are outlined below:

- A **Server-Side Request Forgery attack** against Exchange Server 2013/2016/2019 that allows for authentication as the Exchange server and eventually access the mailbox of any target user. This is a remote exploit against the exposed Exchange Web Server. Specifically, exploitation of this vulnerability involves an HTTP POST request to resources in the **/owa/auth/Current/themes/resources/** URL path on the Exchange server, which does not require authentication to access.
    - Related vulnerability: **CVE-2021-26855**
    - **Note**: The attacker must identify the target domain's Fully Qualified Domain Name (FQDN) for the exploit to work. For networks with only a single Exchange server, the attacker also needs the Domain Security Identifier (SID) for the targeted user; if there are multiple Exchange servers, only the targeted user's email address is required.
- Exploitation of a **Deserialization** in Server 2013/2016/2019 vulnerability that requires Administrator privileges to exploit, which allows an attacker to achieve SYSTEM-level code execution on the target Exchange Server.
    - Related vulnerability: **CVE-2021-26857**
- Two **Arbitrary File Write** vulnerabilities in Exchange Server 2013/2016/2019 that requires Administrator level access and allow the attacker to write data to any location within the exploited server's file system.
    - Related vulnerabilities: **CVE-2021-26858** and **CVE-2021-27065**

Once the attacker has exploited these vulnerabilities and achieved code execution on the target Exchange Server, they begin various post-exploitation activities.

- Deploy web shells for more robust and persistent access to the target. Web shells observed include popular web shells such as **China Chopper** variants and the **ASPXSPY** web shell, as well as custom ASP web shells.
- Dump LSASS using common utilities like **ProcDump** to harvest credentials.
- Compress files for exfiltration using the popular **7-Zip** and **WinRar** utilities.
- Importing Exchange-related **PowerShell snap-ins** to obtain mailbox data from the Exchange Server.
- Using various functionalities of the PowerShell-based **Nishang** hacking tool.
- Performing in memory execution of open-source PowerShell scripts, such as **PowerCat**.
- Usage of **PsExec** for lateral movement.
- Persistence through the addition of **domain user accounts** and alteration of privileges for these accounts.

Technique Detection

Reconnaissance

T1595 – Active Scanning

Attackers engaged in scanning of public IP ranges to discover vulnerable Exchange servers for targeted attacks.

GreyMatter Detections

- RQ-000085-02 - Service Discovery – Inbound
- RQ-000084-02 - Port Scan - Inbound
- RQ-000091-01 - External Scanners

Initial Access

T1190 – Exploit Public-Facing Application

Once a vulnerable server was located, attackers sent several POST requests to the Exchange servers to initiate the exploits, scrape data, upload web shells, and execute remote commands.

GreyMatter Hunts

- HAFNIUM IOC Hunt

Execution

T1059.001 – PowerShell

Following web shell deployment, HAFNIUM operators performed PowerShell commands such as the Nishang **Invoke-PowerShellTcpOneLine** to get an interactive PowerShell reverse connect or bind shell. They also used PowerShell commands to install snap-ins for Exchange, download **PowerCat** from GitHub, and open a connection to a remote server.

GreyMatter Detections

- RQ-SH-000231-03 - PowerShell Malicious Framework Commands
- RQ-SL-000225-02 - PowerShell Hidden Window
- RQ-SM-000224-02 - PowerShell Execution Policy Bypass
- RQ-SM-000229-03 - PowerShell File Download

Persistence

T1505.003 – Server Software Component: Web Shell

The attackers uploaded PHP and ASPX web shells to the Exchange servers to run post-exploitation commands.

GreyMatter Detections

- RQ-SL-000214-03 - IDS Web Shell
- RQ-SM-000251-02 - Web Shell Console Usage
- RQ-SM-000252-02 - Reverse Web Shell Request
- RQ-SL-000253-01 - Suspicious Web Shell Request from Threat Host

Defense Evasion

T1027 – Obfuscated Files or Information

The attackers deployed tools that utilize various PowerShell obfuscation techniques for defense evasion.

GreyMatter Detections

- RQ-SH-000227-01 - PowerShell Obfuscated Script

Credential Access

T1003.001 – LSASS Memory

Once persistent web shells were established, the attackers targeted credentials by dumping LSASS process memory using **ProcDump**. Sample commands provided below:

```
cmd /c cd /d C:\\root&procdump64.exe -accepteula -ma lsass.exe lsass.dmp&echo [S]&cd&echo [E]

C:\Windows\temp\procdump64 -accepteula –ma lsass.exe C:\Windows\temp\lsass
```

GreyMatter Detections

- RQ-SH-000696-01 - Credential Dumping
- RQ-SC-002076-01 - Memory Grab using ProcDump

Discovery

T1016 – System Network Configuration Discovery

Multiple recon commands were executed, including commands using the following utility to discover local system network configuration:

- `ping.exe`

T1007 – System Service Discovery

Multiple recon commands were executed, including commands using the following utility to discover local system services:

- `tasklist.exe`

T1033 – System Owner/User Discovery

Multiple recon commands were executed, including commands using the following utilities to discover local system users:

- `whoami.exe`
- `query.exe`
- `quser.exe`

GreyMatter Detections

- RQ-000119-01 - Recon Commands

Lateral Movement

T1021.002 – Remote Services: SMB/Windows Admin Shares

Attackers used **PSEXEC** to pivot between systems and run remote commands.

GreyMatter Detections

- RQ-SH-000151-04 - PSEXEC Pivoting
- RQ-SM-000782-01 - PSEXEC Process Execution

Collection

T1114.001 – Email Collection: Local Email Collection

Attackers used Exchange PowerShell snap-ins that allowed them to export users' mailbox data. Snap-in and commands leveraging it provided below:

```
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn
Get-Mailbox
Get-MailboxExportRequest –ResultSize 100
Get-MailboxExportRequest | RemoveMailboxExportRequest –Confirm:$false
```

T1560.001 – Archive Collected Data: Archive via Utility

To prepare the stolen data for exfiltration, attackers would compress the data into ZIP files using common utilities such as **7-Zip** and **WinRar**. Sample command provided below:

```
C:\ProgramData\7z a –t7z –r c:\ProgramData\it.zip c:\ProgramData\pst
```

GreyMatter Detections

- RQ-002225-01 - Data Compressed

Command and Control

T1071.001 – Application Layer Protocol: Web Protocols

The attacker leveraged the **Covenant** post-exploitation framework, which commonly uses HTTP(S)-for command and control.

GreyMatter Detections

- RQ-SM-000047-02 - IP Based URL HTTP(S) Request Pattern
- RQ-SM-000049-01 - High Risk Domain HTTP(S) Request Pattern

Exfiltration

T1041 – Exfiltration Over C2 Channel

Since the attacker is utilizing **Covenant** for post-exploitation activities., it's safe to assume that some type of exfiltration occurred over the existing command and control channel.

T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage

Once the attacker has gained access to a victim network, HAFNIUM typically exfiltrates data to file sharing sites like **mega[.]nz**.

GreyMatter Detections

- RQ-SM-000047-02 - IP Based URL HTTP(S) Request Pattern
- RQ-SM-000049-01 - High Risk Domain HTTP(S) Request Pattern

Impact

T1531 – Account Access Removal

The attacker executed a command to delete the 'Administrator' account from the 'Exchange Organization administrators' group. Sample command provided below:

```
cmd /c cd /d C:\\inetpub\\wwwroot\\aspnet_client\\system_web&net group "Exchange Organization administrators" administrator /del /domain&echo [S]&cd&echo [E]
```

GreyMatter Detections

- RQ-000018-01 - Security Group Modifications

ReliaQuest Response

ReliaQuest is approaching the response to this threat campaign from several angles, all supported through our GreyMatter platform.

Intel

The ReliaQuest Threat Management is actively collecting, categorizing, and vetting Indicators of Compromise (IoCs) related to this campaign. All these IoCs are being continuously ingested into the GreyMatter Intel platform for use in investigations by the ReliaQuest SOC and our customer base.

Detect

The ReliaQuest Threat Management team has identified existing Detect artifacts (rules, reports, and dashboards) that can be used to detect the activities associated with this Campaign. We are also engaging our Detection Engineering teams to ensure that these artifacts exist in customer environments, where possible. This ensures that our customer base has a standardized, vetted set of detection rules relevant to the threat.

Additionally, we are performing rapid research and development of detection techniques for new techniques exposed by this threat. In doing so, we are looking to inject even more fine-grained detection capabilities into Detect to address this campaign.

Hunt

If you confirm you had a vulnerable version of on-premises Exchange, the ReliaQuest Analyst team will run a retroactive threat hunt through GreyMatter to identify activity related to the HAFNIUM threat group. These hunts will look for vetted IoCs alongside analysis of identified threat activity.

In addition to these approaches to response, the ReliaQuest Threat Management Team is continuously monitoring the threat campaign for any changes. As new IoCs, behaviors, motivations, and other information about the threat group surfaces, we will provide updates to our customer base and other partners. We will also continue to perform research on adversary tactics, techniques, and procedures to bolster our ability to detect them through Intel, Detect, and Hunt.

Recommendation

In our analysis of the HAFNIUM threat campaign, we've identified some key recommendations to help our customers and partners defend against these attacks:

- Apply the relevant updates from Microsoft to all affected on-premises Exchange Servers (Exchange Server 2013/2016/2019).
- Ensure proper antivirus/endpoint coverage across critical servers, especially on-premises Exchange servers. The adversary in question is using well documented TTPs and well signatured tools for post-exploitation activities.
- Limit remote access to Exchange servers where possible. The chaining of the four vulnerabilities involves remote access to the target Exchange server. Limiting this attack surface is crucial to avoiding compromise.
- Ensure proper logging across your environment, prioritizing the following log sources relevant to the threat campaign:
    - Windows Operating System Logs
    - Endpoint Detection Logs
    - Firewall Logs
    - Forward Proxy Logs
    - Web Server Logs (IIS in particular)
- Search Exchange server logs for indicators of compromise by using Microsoft's prebuilt PowerShell search commands.

References

1. https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
2. https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
3. https://blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day/
4. https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901
5. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
6. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857
7. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858
8. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065