Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities

fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html

Threat Research

Matt Bromiley, Chris DiGiamo, Andrew Thompson, Robert Wallace

Mar 04, 2021

7 mins read

Threat Research

Zero Day Threats

Beginning in January 2021, Mandiant Managed Defense observed multiple instances of abuse of Microsoft Exchange Server within at least one client environment. The observed activity included creation of web shells for persistent access, remote code execution, and reconnaissance for endpoint security solutions. Our investigation revealed that the files created on the Exchange servers were owned by the user NT AUTHORITY\SYSTEM, a privileged local account on the Windows operating system. Furthermore, the process that created the web shell was UMWorkerProcess.exe, the process responsible for Exchange Server's Unified Messaging Service. In subsequent investigations, we observed malicious files created by w3wp.exe, the process responsible for the Exchange Server web front-end.

In response to this activity, we built threat hunting campaigns designed to identify additional Exchange Server abuse. We also utilized this data to build higher-fidelity detections of web server process chains. On March 2, 2021, Microsoft released a blog post that detailed multiple zero-day vulnerabilities used to attack on-premises versions of Microsoft Exchange Server. Microsoft also issued emergency Exchange Server updates for the following vulnerabilities:

CVE	Risk Rating	Access Vector	Exploitability	Ease of Attack	Mandiant Intel
CVE-2021-26855	Critical	Network	Functional	Easy	Link
CVE-2021-26857	Medium	Network	Functional	Easy	Link
CVE-2021-26858	Medium	Network	Functional	Easy	Link
CVE-2021-27065	Medium	Network	Functional	Easy	Link

Table 1: List of March 2021 Microsoft Exchange CVEs and FireEye Intel Summaries

The activity reported by Microsoft aligns with our observations. **FireEye currently tracks this activity in three clusters, UNC2639, UNC2640, and UNC2643. We anticipate additional clusters as we respond to intrusions.** We recommend following Microsoft's guidance and patching Exchange Server immediately to mitigate this activity.

Based on our telemetry, we have identified an array of affected victims including US-based retailers, local governments, a university, and an engineering firm. Related activity may also include a Southeast Asian government and Central Asian telecom. Microsoft reported the exploitation occurred together and is linked to a single group of actors tracked as “HAFNIUM”, a group that has previously targeted the US-based defense companies, law firms, infectious disease researchers, and think tanks.

In this blog post, we will detail our observations on the active investigations we are currently performing. As our experience with and knowledge of this threat actor grows, we will update this post or release new technical details as appropriate. For our Managed Defense Customers, we have launched a Community Protection Event that will provide frequent updates on this threat actor and activity.

We will be discussing these attacks more in an upcoming webinar on Mar. 17, 2021.

From Exploit to Web Shell

Beginning in January 2021, Mandiant Managed Defense observed the creation of web shells on one Microsoft Exchange server file system within a customer’s environment. The web shell, named help.aspx (MD5: 4b3039cf227c611c45d2242d1228a121), contained code to identify the presence of (1) FireEye xAgent, (2) CarbonBlack, or (3) CrowdStrike Falcon endpoint products and write the output of discovery. Figure 1 provides a snippet of the web shell’s code.

Figure 1: Snippet of the web shell help.aspx, crafted to identify the presence of endpoint security software on a victim system

The web shell was written to the system by the UMWorkerProcess.exe process, which is associated with Microsoft Exchange Server’s Unified Messaging service. This activity suggested exploitation of CVE-2021-26858.

Approximately twenty days later, the attacker placed another web shell on a separate Microsoft Exchange Server. This second, partially obfuscated web shell, named iisstart.aspx (MD5: 0fd9bffa49c76ee12e51e3b8ae0609ac), was more advanced and contained functions to interact with the file system. As seen in Figure 2, the web shell included the ability to run arbitrary commands and upload, delete, and view the contents of files.

Snippet of iisstart.aspx, uploaded by the attacker in late January 2021

Figure 2: Snippet of iisstart.aspx, uploaded by the attacker in late January 2021

While the use of web shells is common amongst threat actors, the parent processes, timing, and victim(s) of these files clearly indicate activity that commenced with the abuse of Microsoft Exchange.

In March 2021, in a separate environment, we observed a threat actor utilize one or more vulnerabilities to place at least one web shell on the vulnerable Exchange Server. This was likely to establish both persistence and secondary access, as in other environments. In this case, Mandiant observed the process w3wp.exe, (the IIS process associated with the Exchange web front-end) spawning cmd.exe to write a file to disk. The file, depicted in Figure 3, matches signatures for the tried-and-true China Chopper.

Figure 3: Snippet of China Chopper web shell found on a compromised Exchange Server system

We observed that in at least two cases, the threat actors subsequently issued the following command against the Exchange web server:

```
net group "Exchange Organization administrators" administrator /del /domain.
```

This command attempts to delete the administrator user from the Exchange Organizations administrators group, beginning with the Domain Controller in the current domain. If the system is in a single-system domain, it will execute on the local computer.

Per Microsoft’s blog, they have identified additional post-exploitation activities, including:

- Credential theft via dumping of LSASS process memory.
- Compression of data for exfiltration via 7-Zip.

- Use of Exchange PowerShell Snap-ins to export mailbox data.
- Use of additional offensive security tools Covenant, Nishang, and PowerCat for remote access.

The activity we have observed, coupled with others in the information security industry, indicate that these threat actors are likely using Exchange Server vulnerabilities to gain a foothold into environments. This activity is followed quickly by additional access and persistent mechanisms. As previously stated, we have multiple ongoing cases and will continue to provide insight as we respond to intrusions.

Investigation Tips

We recommend checking the following for potential evidence of compromise:

- Child processes of C:\Windows\System32\inetsrv\w3wp.exe on Exchange Servers, particularly cmd.exe.
- Files written to the system by w3wp.exe or UMWorkerProcess.exe.
- ASPX files owned by the SYSTEM user
- New, unexpected compiled ASPX files in the Temporary ASP.NET Files directory
- Reconnaissance, vulnerability-testing requests to the following resources from an external IP address:
  - /rpc/ directory
  - /ecp/DDI/DDIService.svc/SetObject
  - Non-existent resources
  - With suspicious or spoofed HTTP User-Agents
- Unexpected or suspicious Exchange PowerShell SnapIn requests to export mailboxes

In our investigations to date, the web shells placed on Exchange Servers have been named differently in each intrusion, and thus the file name alone is not a high-fidelity indicator of compromise.

If you believe your Exchange Server was compromised, we recommend investigating to determine the scope of the attack and dwell time of the threat actor.

Furthermore, as system and web server logs may have time or size limits enforced, we recommend preserving the following artifacts for forensic analysis:

- At least 14 days of HTTP web logs from the inetpub\Logs\LogFiles directories (include logs from all subdirectories)
- The contents of the Exchange Web Server (also found within the inetpub folder)
- At least 14 days of Exchange Control Panel (ECP) logs, located in Program Files\Microsoft\Exchange Server\v15\Logging\ECP\Server
- Microsoft Windows event logs

We have found significant hunting and analysis value in these log folders, especially for suspicious CMD parameters in the ECP Server logs. We will continue updating technical details as we observe more related activity.

Technical Indicators

The following are technical indicators we have observed, organized by the threat groups we currently associate with this activity. To increase investigation transparency, we are including a Last Known True, or LKT, value for network indicators. The LKT timestamp indicates the last time Mandiant knew the indicator was associated with the adversary; however, as with all ongoing intrusions, a reasonable time window should be considered.

UNC2639

Indicator	Type	Note
165.232.154.116	Network: IP Address	Last known true: 2021/03/02 02:43
182.18.152.105	Network: IP Address	Last known true: 2021/03/03 16:16

UNC2640

Indicator	Type	MD5
help.aspx	File: Web shell	4b3039cf227c611c45d2242d1228a121
iisstart.aspx	File: Web shell	0fd9bffa49c76ee12e51e3b8ae0609ac

UNC2643

Indicator	Type	MD5/Note
Cobalt Strike BEACON	File: Shellcode	79eb217578bed4c250803bd573b10151
89.34.111.11	Network: IP Address	Last known true: 2021/03/03 21:06
86.105.18.116	Network: IP Address	Last known true: 2021/03/03 21:39

Detecting the Techniques

FireEye detects this activity across our platforms. The following contains specific detection names that provide an indicator of Exchange Server exploitation or post-exploitation activities we associated with these threat actors.

Platform(s)	Detection Name
• Network Security • Email Security • Detection On Demand • Malware File Scanning • Malware File Storage Scanning	• FEC_Trojan_ASPX_Generic_2 • FE_Webshell_ASPX_Generic_33 • FEC_APT_Webshell_ASPX_HEARTSHELL_1 • Exploit.CVE-2021-26855
Endpoint Security	**Real-Time (IOC)** • SUSPICIOUS CODE EXECUTION FROM EXCHANGE SERVER (EXPLOIT) • ASPXSPY WEBSHELL CREATION A (BACKDOOR) • PROCDUMP ON LSASS.EXE (METHODOLOGY) • TASKMGR PROCESS DUMP OF LSASS.EXE A (METHODOLOGY) • NISHANG POWERSHELL TCP ONE LINER (BACKDOOR) • SUSPICIOUS POWERSHELL USAGE (METHODOLOGY) • POWERSHELL DOWNLOADER (METHODOLOGY) **Malware Protection (AV/MG)** Trojan.Agent.Hafnium.A **Module Coverage** [Process Guard] - prevents dumping of LSASS memory using the procdump utility.
Helix	• WINDOWS METHODOLOGY [Unusual Web Server Child Process] • MICROSOFT EXCHANGE [Authentication Bypass (CVE-2021-26855)]