Multiple Microsoft Exchange zero-day vulnerabilities: HAFNIUM campaign

20210304

Vulnerability Overview

On March 2, 2021, the Microsoft Threat Intelligence Center (MSTIC) released details on an active state-sponsored threat campaign, which is leveraging four zero-day vulnerabilities to attack on-premise instances of Microsoft Exchange Server.

In the attacks observed by Microsoft, the threat actor used the vulnerabilities to access on-premise Exchange servers, enabling them to access email accounts and allowing installation of additional malware to facilitate persistent access to victim environments. Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to HAFNIUM, a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures.

The zero-day vulnerabilities disclosed on March 2, 2021, are:

- **CVE-2021-26855** is a server-side request forgery (SSRF) vulnerability in Exchange that allows an attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
- **CVE-2021-26857** is an insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is deserialized by a program. Exploiting this vulnerability gave HAFNIUM the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to exploit.
- **CVE-2021-26858** is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.
- **CVE-2021-27065** is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability to

write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.

For the latest crowd-sourced information on the vulnerabilities, check the AttackerKB page.

Exploitation

These vulnerabilities are being actively exploited in the wild.

On March 2, Microsoft stated that the observed attacks were "limited and targeted." However, Rapid7 detection and response teams have been detecting **indiscriminate exploitation of Exchange servers since February 27, 2021**, including but not limited to the attacker behaviors below:

- Attacker Tool – China Chopper Webshell Executing Commands
- Attacker Technique – ProcDump Used Against LSASS

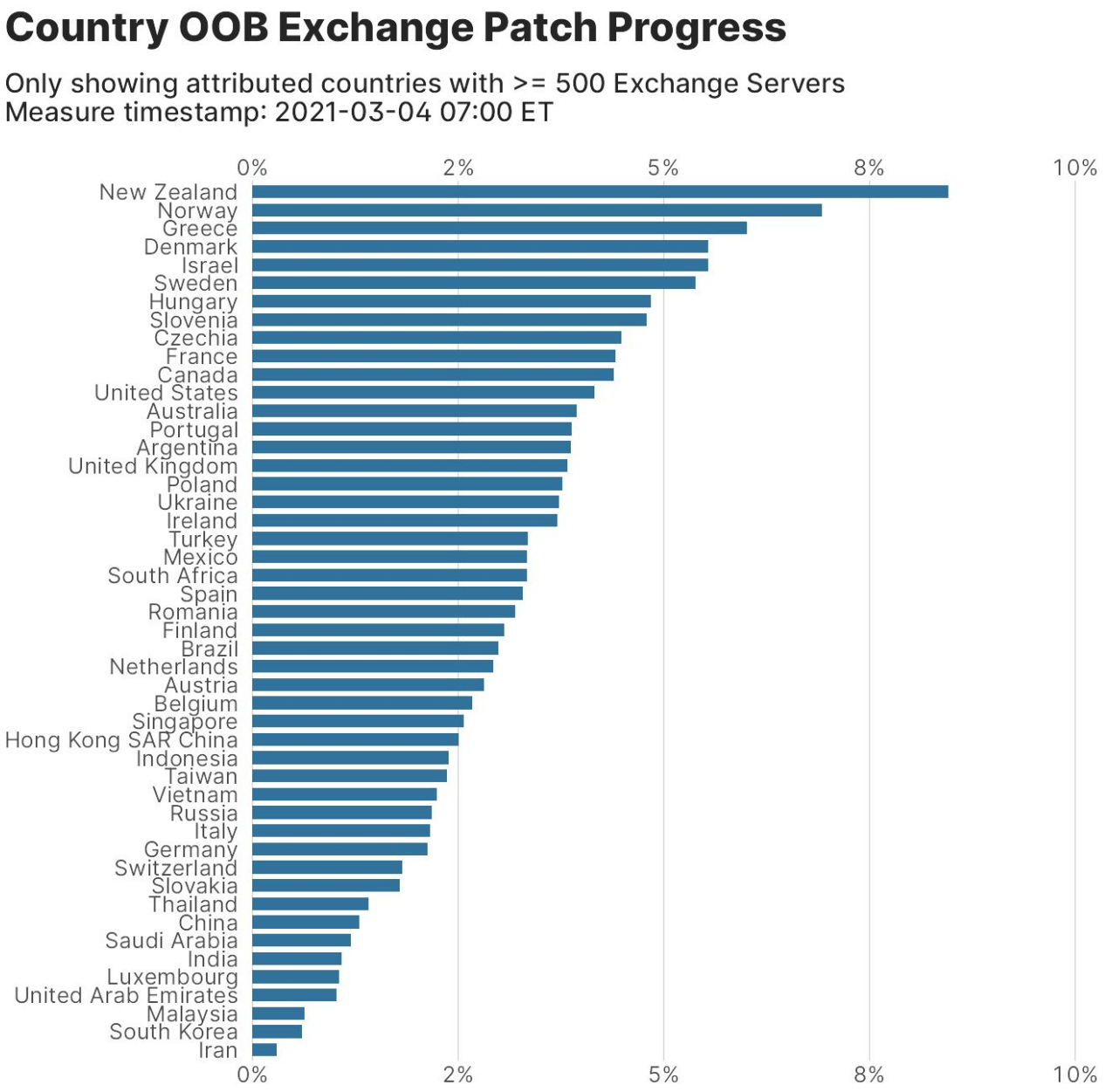
More information on attacker behaviors and a timeline of widespread Exchange exploitation is available here.

There are some commonalities across attacker groups attempting to use this vulnerability to gain a foothold within an organization. The following files have been seen present in multiple, compromised environments can can be tested for with unauthenticated HTTP requests to the following paths:

- `/owa/auth/document.aspx`
- `/owa/auth/errorEE.aspx`
- `/owa/auth/web.aspx`
- `/owa/auth/help.aspx`
- `/owa/auth/document.aspx`
- `/owa/auth/errorEE.aspx`
- `/owa/auth/errorEEE.aspx`
- `/owa/auth/errorEW.aspx`
- `/owa/auth/errorFF.aspx`
- `/owa/auth/healthcheck.aspx`
- `/owa/auth/web.aspx`
- `/owa/auth/help.aspx`

Exposure

As of Thursday, March 4, 2021, at 07:00 ET less than ~11.5% of internet-facing exchange systems (~350K total) were patched. No single country with 500 or more Exchange servers deployed has more than 9% of systems patched.



Recommended Next Steps

Microsoft has released out-of-band patches for all four vulnerabilities as of March 2, 2021, and Rapid7 strongly recommends deploying patches immediately.

Microsoft Exchange customers should apply the latest updates on an emergency basis and take steps to harden their Exchange instances. We strongly recommend that organizations monitor closely for suspicious activity and indicators of compromise (IOCs) stemming from this campaign. Rapid7 has a comprehensive list of IOCs available here.

For further information on the HAFNIUM-attributed threat campaign and related IOCs, see Microsoft's blog here: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Affected products

- Exchange Server 2013
- Exchange Server 2016
- Exchange Server 2019

Security updates are available for the following specific versions of Exchange:

- Exchange Server 2010 (for Service Pack 3 – this is a Defense in Depth update)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

Exchange Online is not affected.

For more information, or to obtain data specific to your organization, region, or sector, please contact research@rapid7.com.