China-backed Threat Actor Hafnium Exploiting Four Microsoft Exchange Zero-Days

Vulnerability Bulletins **TLP:WHITE** **Alert Id: 7644b423** **2021-03-05 16:25:22**

On March 2, 2021, Microsoft published "New nation-state cyberattacks" on their blog. The post focuses on Hafnium, a highly skilled and sophisticated threat actor operating from China. While Hafnium is based in China, it conducts operations primarily from leased virtual private servers (VPS) in the United States.

Microsoft has detected multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. In the attacks observed, the threat actor used these vulnerabilities to access on-premises Exchange servers which enabled access to email accounts and allowed installation of additional malware to facilitate long-term access to victim environments.

The vulnerabilities observed being exploited are:

- CVE-2021-26855
- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065

In response, Microsoft has released security updates that will protect customers running Exchange Server and has also made their Microsoft EMEA Out of Band Webcast presentation available here. Additionally, Microsoft briefed appropriate agencies on this activity. Microsoft has provided additional information including technical details, host IOCs, attack details, and mitigation strategies made available here.

Health-ISAC's Threat Operations Center (TOC) will continue to monitor developments as they become available. Additionally, Health-ISAC's Threat Operations Center has created a HAFNIUM PowerPoint presentation for members which is available in the Health-ISAC Threat Portal Doc Library for download. The PowerPoint will continue to be updated accordingly.

Reference(s): Microsoft, Microsoft, Microsoft, Health-ISAC

Recommendations:

Promptly applying patches is the best protection against this attack. Microsoft has released security updates that will protect customers running Exchange Server.

Sources:

Bleeping Computer - Microsoft Fixes Actively Exploited Exchange Zero-day Bugs, Patch Now
Microsoft Blog - New Nation-State Cyberattacks
TechCrunch - Microsoft Says China-Backed Hackers Are Exploiting Exchange Zero-Days
Microsoft: Multiple Security Updates Released for Exchange Server
HAFNIUM targeting Exchange Servers with 0-day exploits
Microsoft: Released: March 2021 Exchange Server Security Updates
Volexity: Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities

Tags: HAFNIUM

For Questions or Comments: Please email us at toc@h-isac.org