Microsoft releases updates to patch vulnerabilities actively exploited in Microsoft Exchange

Dear Constituents,

Microsoft has released an emergency out-of-band security updates for all supported Microsoft Exchange versions that fix four zero-day vulnerabilities actively exploited in targeted attacks. Threat actors have been observed primarily targeting entities in the United States for the purpose of exfiltrating information from a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks and NGOs.

How it works

In order for this attack to work, remote attackers would need to access an on premise Microsoft Exchange server on port 443. If access is available, the threat actors would then utilize the following vulnerabilities to gain remote access. The four vulnerabilities are:

1. CVE-2021-26855, a server-side request forgery (SSRF) vulnerability that allowed the attackers to send arbitrary HTTP requests and authenticate as the Exchange server.

2. CVE-2021-26857, an insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is when 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.

3. CVE-2021-26858, a post-authentication arbitrary file write vulnerability. If threat actors could authenticate with the Exchange server, then it could use this vulnerability to write a file to any path on the server. The group could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.

4. CVE-2021-27065, a post-authentication arbitrary file write vulnerability. If the adversaries could authenticate with the Exchange server, they could use this vulnerability to write a file to any path on the server. It could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials

---

Systems affected

- Microsoft Exchange Server 2010 RU31 for Service Pack 3

- Microsoft Exchange Server 2013 CU 23

- Microsoft Exchange Server 2016 CU 18, CU 19

- Microsoft Exchange Server 2019 CU 7, CU 8

What to do

1. It is recommended prioritize installing updates on Exchange Servers that are externally facing.

2. All affected Exchange Servers should ultimately be updated

3. Please use best practice in applying patches and updates

Reference

- https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

For more information please contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
Email: cert@cert.gov.to
Web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga