TLP: White[1]

Vulnerabilities Actively Exploited in Microsoft Exchange

(Updated 12th March 2021, 5:30pm)

Dear Constituents,

This is our updated advisory regarding the above and should supersede our advisory issued on 10 March 2021. As this is an ongoing incident those of you affected by this should continuously monitor for updates from the vendor on the link provided below under Reference.

We have received reports that this ongoing attack is now linked to threat actors encrypting victims' data for ransom otherwise known as ransomware. This is in addition to compromising networks and stealing information.

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 wide-spread attacks. Microsoft continues to see multiple actors taking advantage of unpatched systems to attack organizations with on-premises Exchange Server. They also released tools to assist with mitigation and detection of a compromise which can be found here: *https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/*

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 gives threat actors 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

1 CERT Tonga adopts the Traffic Light Protocol

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

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

What to do

1. Urgently backup your data and ensure your backups are tested.
2. All affected Exchange Servers should ultimately be patched ensuring the User Account Control (UAC) is disabled before applying the updates.
3. If unable to patch, follow the instruction provided here: *https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/*
4. 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

entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services