Ministry of Meteorology Energy
Information, Disaster Management,
Environment, Communications and
Climate Change

TLP: Green[1]

Vulnerabilities Actively Exploited in Microsoft Exchange (Supplement)

Dear Constituents,

This is a supplement to our previous advisory that we have issued on 12th March 2021, regarding the vulnerabilities exploited in Microsoft Exchange Server. As this is an ongoing attack, those of you affected by this should continuously monitor for updates from the vendor on the link provided below under Reference.

CERT Tonga is still receiving reports of this ongoing attack which is now linked to different threat actors encrypting victims' data for ransom otherwise known as ransomware. This is in addition to compromising networks and stealing Information (credentials and emails).

Please be advised that this advisory is **TLP: GREEN**, which means that you can share this advisory with peers and partner organizations within your sector or community, but not via publicly accessible channels.

What to do

This is in addition to steps provided in our previously issued advisory. Be sure to take the most appropriate steps below:

- **To those who have not yet patched**: Microsoft has now released a new, one-click mitigation tool, Microsoft Exchange On-Premises Mitigation Tool to help users who do not have dedicated security or IT teams to apply these security updates.

  This new tool is designed as an interim mitigation for customers who are unfamiliar with the patch/update process or who have not yet applied the on-premises Exchange security update: https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/

[1] CERT Tonga adopts the Traffic Light Protocol

- **For those who needs an interim solution before applying updates**: Microsoft are providing the following mitigation techniques to help customers who need more time to patch their deployments and are willing to make risk and service function trade-offs: https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

- **For those who have patched**: Microsoft has updated their Microsoft Safety Scanner (MSERT) tool to find and remove malware as well as trying to reverse changes made by identified threats. It also discovers and remediates web shells, which are backdoors that adversaries use to maintain persistence on your server: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

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

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal 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