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

TLP: White[1]

Microsoft Exchange Vulnerability

Dear Constituents,

A vulnerability on affected installations of Microsoft Exchange Server is currently being exploited which allows remote attackers to execute code in those systems.

How it Works

This attack requires network access to the Exchange Control Panel (ECP) with valid set of Exchange credentials. Note that all that is required is a Domain User account, not an Exchange Admin.

The specific flaw exists within the Exchange Control Panel (ECP) web application. The product fails to generate a unique cryptographic key at installation, which can result in deserialization of untrusted data. The attacker can leverage this vulnerability to execute code in the context of SYSTEM.

What to do

- It is highly recommended to apply the February 2020 security updates immediately
- Restrict network access to the ECP.
- Enable Multi-Factor Authentication (MFA) on the Exchange Server.

Reference

- Microsoft: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688
- CERT Tonga: https://www.cert.gov.to/wp-content/uploads/2020/02/Patch-Tuesday-February-2020.pdf

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to

1 CERT Tonga adopts the Traffic Light Protocol

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