CERT Tonga

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

TLP: White[1]

Remote Code Execution Vulnerability in Microsoft SMBv3

Dear Constituents,

Microsoft has released a security advisory to address a remote code execution vulnerability in **Microsoft Server Message Block** 3.1.1 (SMBv3). SMB is a network file-sharing protocol that allows client machines to access files on servers.

Some of the major ransomware infections, has been the consequence of SMB-based exploits which was used in the WannaCry and NotPetya ransomware which spread globally through a worm-like behavior in 2017.

At the time of drafting this advisory, Microsoft had not release an update to patch this vulnerabilitiy. As such, constituents are encouraged to look out for this patch and update once it becomes available.

How it Works

To exploit the vulnerability against an SMB Server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 Server. To exploit the vulnerability against an SMB Client, an unauthenticated attacker would need to configure a malicious SMBv3 Server and convince a user to connect to it.

What to do

- Disable TCP port 445 on firewalls and client computers.
- Disable SMBv3 compression to block unauthenticated attackers from exploiting the vulnerability against the SMBv3 Server.
- It is strongly recommends installing the updates for this vulnerability as soon as they become available.

Reference

- Microsoft- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv200005

Please for more information you can contact us:

1 CERT Tonga adopts the Traffic Light Protocol

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

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