CERT Tonga

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

TLP: White[1]

Microsoft Netlogon Vulnerability

Dear Constituents,

An exploit has been released related to a vulnerability found in Microsoft Netlogon which is a protocol that authenticates users and machines in domain-based networks and is also used to update computer passwords remotely. By exploiting this vulnerability, an attacker can hijack a domain controller in which the following Window server versions are affected:

- Windows Server 2019
- Windows Server 2016
- Windows Server version 1909
- Windows Server version 1903
- Windows Server version 1809
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 Service Pack 1

How it works

The attacker can impersonate a client computer and replace the password of a domain controller (a server that controls an entire network and runs Active Directory services). This leads the attacker to gain domain administration rights to that particular Window Server.

What to do

Microsoft has released a guideline in the link below on how to manage the changes in Netlogon secure channel connections associated with this vulnerability- https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

Reference

Microsoft- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

[1] CERT Tonga adopts the Traffic Light Protocol

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