CERT Tonga

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

**TLP: White**[1]

# Security Bulletin – June 2020

Dear Constituents,

Please find below our monthly roundup of security vulnerabilities for your information and necessary actions to secure your network and assets.

## Vulnerabilities with Active Exploits in the Wild

### Exim Remote Command Execution Vulnerability *(CVE-2019-10149)* Severity: HIGH

Exim is exposed to a remote command execution vulnerability. Successfully exploiting this issue may allow an attacker to execute arbitrary commands as root.

#### How it works

Exploitation of the vulnerability only requires a malicious email to be sent to a vulnerable server, and injected commands will typically run as root. There are multiple ways that Exim can be configured, and some of these will allow for faster exploitation, while others may require a week to fully exploit.

#### What to do

Apply appropriate updated version recommended by the Vendor

#### Reference

https://www.exim.org/static/doc/security/CVE-2019-10149.txt

### WordPress BBPress Privilege Escalation Vulnerability *(CVE-2020-13693)* Severity: HIGH

An unauthenticated privilege escalation issue exists in the BBPress plugin for WordPress when New User Registration is enabled.

#### How it works

Attackers who exploit the logic bug could grant themselves authorization to delete forum activities, import or export forum users, and create new forum moderators, according to the security researcher who discovered the flaw.

Attackers can simply add the bbp-forums-role parameter with the value of bbp_keymaster to the signup request, you can effectively make the newly created user a ‘Keymaster’ which is a forum administrator, gaining complete forum control.

[1] CERT Tonga adopts the Traffic Light Protocol

#### What to do

Apply appropriate updated version required by the Vendor (version 2.6.5)

#### Reference

https://portswigger.net/daily-swig/wordpress-security-critical-flaw-fixed-in-bbpress-forum-pluginps://packetstormsecurity.com/files/157885/WordPress-BBPress-2.5-Privilege-Escalation.html

https://bbpress.org/blog/2020/05/bbpress-2-6-5-is-out/

### **Windows SMB Authenticated Remote Code Execution Vulnerability** *( CVE-2020-1301, CVE 1206)* Severity: **HIGH**

For Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 operating systems, a remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests when an authenticated attacker sends specially crafted packets to the SMBv1 server. The vulnerability does not impact other SMB Server versions.

#### How it works

On later operating systems, an attacker who successfully exploited this vulnerability could cause the affected system to stop responding until it is manually restarted.

An attacker would need to authenticate to the SMBv1 Server and have permission to open files on the target server before attempting the attack.

#### What to do

Apply appropriate security updates and patch as recommended by Microsoft

#### Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1301

## Other Vulnerabilities with known Exploits

### **VMware Cloud Director Code Injection Vulnerability** *( CVE-2020-3956)* Severity: **MEDIUM**

Description: VMware Cloud Director do not properly handle input leading to a code injection vulnerability. An authenticated actor may be able to send malicious traffic to VMware Cloud Director which may lead to arbitrary remote code execution. This vulnerability can be exploited through the HTML5- and Flex-based UIs, the API Explorer interface and API access.

### **Microsoft splwow64 Elevation of Privilege Vulnerability** *( CVE-2019-0880)* Severity: **MEDIUM**

Description: A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls. An attacker who successfully exploited the vulnerability could elevate privileges on an affected system from low-integrity to medium-integrity. This vulnerability by itself does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability (such as a remote code execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted.

## Other Vulnerabilities

### Docker Engine IPv6 Address Spoofing Vulnerability ( *CVE-2020-11022)* Severity: MEDIUM

Description: An issue exists in Docker Engine where an attacker in a container, with the CAP_NET_RAW capability, can craft IPv6 router advertisements, and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service. A user is able to create containers with CAP_NET_RAW privileges on an affected cluster can intercept traffic from other containers on the host or from the host itself.

Compiled with information from SANS' @RISK: The Concensus Security Vulnerability Alerts.

The Severity ratings on the above vulnerabilities are based on the NIST Common Vulnerability Scoring System Calculator (CVSS) version 2.

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