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

**TLP: White**[1]

# Security Bulletin – September 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

### **Linux Kernel Denial of Service Vulnerability** *(CVE-2020-14356)* Severity: **HIGH**

#### Description

A flaw null pointer dereference in the Linux kernel cgroupv2 subsystem was found in the way when reboot the system.

#### How it works

A local user could use this flaw to crash the system or escalate their privileges on the system. Successful exploitation of this vulnerability could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service.

#### What to do

Ensure to apply appropriate security patch as recommended.

#### Reference

https://bugzilla.kernel.org/show_bug.cgi?id=208003

https://lore.kernel.org/netdev/CAM_iQpUKQJrj8wE+Qa8NGR3P0L+5Uz=qo-O5+k_P60HzTde6aw%40mail.gmail.com/t/

### **Microsoft Exchange Server Remote Code Execution Vulnerability** *(CVE-2020-16875)* Severity: **HIGH**

#### Description

A remote code execution vulnerability exists in Microsoft Exchange server due to improper validation of cmdlet arguments.

#### How it works

An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user. Exploitation of the vulnerability requires an authenticated user in a certain Exchange role to be compromised.

[1] CERT Tonga adopts the Traffic Light Protocol

### What to do

Ensure to apply appropriate security updates recommended by Microsoft.

### Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16875

## PAN-OS Management Interface Command Injection Vulnerability *(CVE-2020-0986, CVE-2020-2037)* Severity: HIGH

### Description

An OS Command Injection vulnerability exists in the PAN-OS management interface.

### How it works

It allows authenticated administrators to execute arbitrary OS commands with root privileges. This issue affects some unknown processing of the component Management Interface. The manipulation with an unknown input leads to a privilege escalation vulnerability.

### What to do

This issue is fixed in PAN-OS 8.1.16, PAN-OS 9.0.10, PAN-OS 9.1.3, and all later PAN-OS versions

### Reference

https://security.paloaltonetworks.com/CVE-2020-2037

## vBulletin Remote Code Execution Vulnerability *(CVE-2020-17496)* Severity: HIGH

### Description

A vulnerability found and could be exploited by the attackers in vBulletin

### How it works

vBulletin 5.5.4 through 5.6.2 allows remote command execution by attacker via crafted subWidgets data in an ajax/render/widget_tabbedcontainer_tab_panel request.

NOTE: this issue exists because of an incomplete fix for CVE-2019-16759 shown in August 2020 Security Bulletin

### What to do

Ensure to apply appropriate patch available for the following versions of vBulletin:

- 5.6.2
- 5.6.1
- 5.6.0

### Reference

https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4445227-vbulletin-5-6-0-5-6-1-5-6-2-security-patch

https://blog.exploitee.rs/2020/exploiting-vbulletin-a-tale-of-patch-fail/

## **Microsoft Win32k Elevation of Privilege Vulnerability** *(CVE-2020-1247)* Severity: **HIGH**

### Description

An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory.

### How it works

An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

### What to do

Ensure to apply appropriate security updates recommended by Microsoft.

### Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1247

## **Microsoft Windows Kernel Elevation of Privilege Vulnerability** *(CVE-2020-0986)* Severity: **HIGH**

### Description

An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory.

### How it works

An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system.

### What to do

Ensure to apply appropriate security updates recommended by Microsoft.

### Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0986

## **Cisco Jabber for Windows Message Handling Arbitrary Code Execution Vulnerability** *(CVE-2020-3495)* Severity: **HIGH**

### Description

A vulnerability in Cisco Jabber for Windows could allow an authenticated, remote attacker to execute arbitrary code.

### How it works

The vulnerability is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted Extensible Messaging and Presence Protocol (XMPP) messages to the affected software. A successful exploit could allow the attacker to cause the application to execute arbitrary programs on the targeted system with the privileges of the user account that is running the Cisco Jabber client software, possibly resulting in arbitrary code execution.

### What to do

Cisco has release the software updates that address the vulnerability.

### Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-UyTKCPGg

## Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerabilities *(CVE-2020-3566)*

Severity: **HIGH**

### Description

Multiple vulnerabilities in the Distance Vector Multicast Routing Protocol (DVMRP) feature of Cisco IOS XR Software

### How it works

It could allow an unauthenticated, remote attacker to either immediately crash the Internet Group Management Protocol (IGMP) process or make it consume available memory and eventually crash. The memory consumption may negatively impact other processes that are running on the device.

These vulnerabilities are due to the incorrect handling of IGMP packets. An attacker could exploit these vulnerabilities by sending crafted IGMP traffic to an affected device. A successful exploit could allow the attacker to immediately crash the IGMP process or cause memory exhaustion, resulting in other processes becoming unstable.

### What to do

Cisco has release the software updates that address the vulnerability.

### Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz

## IBM WebSphere Application Server Remote Code Execution Vulnerability *(CVE-2020-4589)*

Severity: **HIGH**

### Description

WebSphere Application Server is vulnerable to a remote code execution vulnerability. This has been addressed.

### How it works

IBM WebSphere Application Server could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources.

### What to do

Ensure to apply appropriate security updates recommended by IBM

### Reference

https://exchange.xforce.ibmcloud.com/vulnerabilities/184585

https://www.ibm.com/support/pages/node/6258333

## Other Vulnerabilities with known Exploits

**Apache OFBiz XML-RPC Cross-Site Scripting Vulnerability** (CVE-2020-9496*)* Severity: **MEDIUM**

Description: Apache OFBiz XML-RPC request are vulnerable to unsafe deserialization and Cross-Site Scripting vulnerability.

**BitTorrent uTorrent Denial of Service Vulnerability** (CVE-2020-8437*)* Severity: **MEDIUM**

Description: The bencoding parser in BitTorrent uTorrent misparses nested bencoded dictionaries, which allows a remote attacker to cause a denial of service.

**IBM QRadar Arbitrary File Overwrite Vulnerability** (CVE-2020-4486*)* Severity: **MEDIUM**

Description: IBM QRadar allows an authenticated user to overwrite or delete arbitrary files due to a flaw after WinCollect installation.

**Linux kernel "af_packet.c" Memory Corruption Vulnerability** (CVE-2020-14386*)* Severity: **MEDIUM**

Description: A Memory corruption vulnerability exists in the Linux kernel that can be exploited to gain root privileges from unprivileged processes. The highest threat from this vulnerability is to data confidentiality and integrity.

**Pulse Connect Secure Arbitrary Code Execution Vulnerability** (CVE-2020-8218*)* Severity: **MEDIUM**

Description: A code injection vulnerability exists in Pulse Connect Secure that allows an attacker to crafted a URI to perform an arbitrary code execution via the admin web interface.

**Google Android Play Core Library Arbitrary Code Execution Vulnerability** (CVE-2020-8913*)* Severity: **MEDIUM**

Description: A local, arbitrary code execution vulnerability exists in the SplitCompat.install endpoint in Android's Play Core Library. A malicious attacker could create an app which targets a specific application, and if a victim were to install this app, the attacker could perform a directory traversal, execute code as the targeted application and access the targeted application's data on the Android device.

### **Oracle VM VirtualBox Arbitrary Code Execution Vulnerability** *(CVE-2020-2674)* Severity: **MEDIUM**

Description:  Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox.

### **Cisco NX-OS Software Border Gateway Protocol Multicast VPN Session Denial of Service Vulnerability** *(CVE-2020-3398)* Severity: **MEDIUM**

Description: A vulnerability in the Border Gateway Protocol (BGP) Multicast VPN (MVPN) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a BGP session to repeatedly reset, causing a partial denial of service condition due to the BGP session being down. The vulnerability is due to incorrect parsing of a specific type of BGP MVPN update message. An attacker could exploit this vulnerability by sending this BGP MVPN update message to a targeted device. A successful exploit could allow the attacker to cause the BGP peer connections to reset, which could lead to BGP route instability and impact traffic.

### **Microsoft Windows Hyper-V Denial of Service Vulnerability** *(CVE-2020-0751)* Severity: **LOW**

Description: A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.

## Other Vulnerabilities

### MobileIron Core and Connector Remote Code Execution Vulnerability *(CVE-2020-15505)*

Description: A remote code execution vulnerability exists in MobileIron Core and Connector, and Sentry, that allows remote attackers to execute arbitrary code via unspecified vectors. The manipulation with an unknown input leads to a privilege escalation vulnerability.

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 2.0

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