CERT Tonga

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

TLP: White[1]

Security Bulletin – March 2022

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

Information disclosure vulnerability in TIBCO BusinessConnect Container Edition (*CVE-2021-43049)* Severity: **HIGH**

Description

A vulnerability found a database component of TIBCO Software Inc.'s TIBCO BusinessConnect Container Edition.

How it works

It contains an easily exploitable vulnerability that allows an unauthenticated attacker with network access to obtain the usernames and passwords of users of the affected system

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://www.tibco.com/support/advisories/2022/01/tibco-security-advisory-february-15-2022-tibco-bcce-2021-43049

Command injection vulnerability in Xiaomi Router AX3600 (*CVE-2021-14115)* Severity: **HIGH**

Description

A command injection vulnerability exists in the Xiaomi Router AX3600. The vulnerability is caused by a lack of inspection for incoming data detection.

[1] CERT Tonga adopts the Traffic Light Protocol

How it works

Attackers can exploit this vulnerability to execute code.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=37

Command injection vulnerability in Zyxel NWA-1100-NH firmware *(CVE-2021-4039)*

Severity: **HIGH**

Description

A command injection vulnerability in the web interface of the Zyxel NWA-1100-NH firmware.

How it works

could allow an attacker to execute arbitrary OS commands on the device.

What to do

Make sure that you apply the appropriate updates recommended by Vendor.

Reference

https://www.zyxel.com/support/OS-command-injection-vulnerability-of-NWA1100-NH-access-point.shtml

Remote code execution vulnerability in TP-Link Tapo C200 IP camera *(CVE-2021-4045)* Severity: **HIGH**

Description

TP-Link Tapo C200 IP camera, on its 1.1.15 firmware version and below, is affected by an unauthenticated RCE vulnerability, present in the uhttpd binary running by default as root.

How it works

The exploitation of this vulnerability allows an attacker to take full control of the camera.

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://www.incibe-cert.es/en/early-warning/security-advisories/tp-link-tapo-c200-remote-code-execution-vulnerability

Buffer overflow vulnerability in TP-LINK WR-886N 20190826 2.3.8 (*CVE-2021-44622, CVE-2021-44623, CVE-2021-44625, CVE-2021-44626, CVE-2021-44627, CVE-2021-44628, CVE-2021-44630, CVE-2021-446231*, *CVE-2021-446232)* Severity: **HIGH**

Description

A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 in the /cloud_config/router_post/check_reg_verify_code function.

How it works

This code fucntion could allow a remote malicious user to execute arbitrary code via a crafted post request.

What to do

Make sure that you apply the most appropriate updates recommended by TP-Link.

Reference

https://github.com/Yu3H0/IoT_CVE/tree/main/886N/chkRegVeriRegister

Other Vulnerabilities with known Exploits

Out-of-bounds read vulnerability in the IFAA module (*CVE-2021-40050)* Severity: **MEDIUM**

Description: Successful exploitation of this vulnerability may cause stack overflow.

Compiled with information from SANS' @RISK: The Consensus 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.