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

TLP: White[1]

Security Bulletin – July 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

Google Android permission vulnerability (CVE-2022-20216, CVE-2022-20222) Severity: **HIGH**

Description

The vulnerability exists due to improperly imposed security restrictions in Unisoc Telephony component.

How it works

A local application can execute arbitrary code with elevated privileges. The vulnerability affects the Google Android versions: 10 - 10 2022-07-01, 11 - 11 2022-07-01, 12 - 12L 2022-07-01

What to do

Apply the appropriate updates as recommended by Google Android

Reference

https://source.android.com/security/bulletin/2022-07-01

Remote code execution and denial of service vulnerability in Cisco Small Business Routers (*CVE-2022-20825)* Severity: HIGH

Description

A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W.

How it works

1 CERT Tonga adopts the Traffic Light Protocol

Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause an affected device to restart unexpectedly, resulting in a denial of service (DoS) condition.

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-overflow-s2r82P9v

Remote code execution vulnerability in Dell EMC Storage (*CVE-2022- 31446)* Severity: **HIGH**

Description

Cloud Mobility for Dell EMC Storage, 1.3.0.XXX contains an RCE vulnerability.

How it works

A non-privileged user could potentially exploit this vulnerability, leading to achieving a root shell. This is a critical issue.

What to do

Dell recommends users to upgrade at the earliest opportunity.

Reference

https://www.dell.com/support/kbdoc/en-us/000201258/dsa-2022-182-cloud-mobility-for-dell-emc-storage-security-update-for-a-path-traversal-rce-vulnerability

Memory corruption vulnerability in Qualcomm Snapdragon Auto DSM Packet (CVE-2021-30341, CVE-2021-35104*)* Severity: **HIGH**

Description

A vulnerability found in in Qualcomm Snapdragon Auto DSM Packet and Flac auto Clip

How it works

Improper buffer size validation of DSM packet received can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://www.qualcomm.com/company/product-security/bulletins/april-2022-bulletin

Buffer overflow vulnerability in Infiray IRAY-A8Z3 1.0.957 strcpy (CVE-2022-31209, CVE-2022-31211) Severity: **HIGH**

Description

An issue was discovered in Infiray IRAY-A8Z3 1.0.957.

How it works

The firmware contains a potential buffer overflow by calling strcpy() without checking the string length beforehand. Manipulation with an unknown input can lead to a memory corruption vulnerability.

What to do

Please do ensure that you apply the most appropriate updates recommended.

Reference

https://sec-consult.com/vulnerability-lab/advisory/infiray-iray-thermal-camera-multiple-vulnerabilities/

Remote code execution vulnerability in Roxy-WI (*CVE-2022-31137)* Severity: **HIGH**

Description

Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Versions prior to 6.1.1.0 are subject to a remote code execution vulnerability.

How it works

System commands can be run remotely via the subprocess_execute function without processing the inputs received from the user in the /app/options.py file. Attackers need not be authenticated to exploit this vulnerability.

What to do

Users are advised to upgrade. There are no known workarounds for this vulnerability.

Reference

https://github.com/hap-wi/roxywi/commit/82666df1e60c45dd6aa533b01a392f015d32f755

Password authentication flaw in the multiple Lenze products (*CVE-2022-2302)* Severity: **HIGH**

Description

The machine controller of the cabinet series include an OPC-UA server which uses an user management to authenticate clients via anonymous or user/password authentication.

How it works

If the user/password authentication is selected, password verification is skipped upon second login. As a result, cases occur in which users can establish communication without correct authentication. This vulnerability is not located in the OPC-UA protocol or server, but in the interface to the products firmware.

What to do

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

Reference

https://cert.vde.com/en/advisories/VDE-2022-030/

Path traversal vulnerability in CWP v0.9.8.1122 (*CVE-2022-25046)* Severity: **HIGH**

Description

A Vulnerabilities found in CWP

How it works

A path traversal vulnerability in loader.php of CWP v0.9.8.1122 allows attackers to execute arbitrary code via a crafted POST request.

What to do

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

Reference

https://github.com/Immersive-Labs-Sec/CentOS-WebPanel

Other Vulnerabilities with known Exploits

Out-of-bounds write in Modem 2G RR (CVE-2022-21744, CVE-2022-20083) Severity: **MEDIUM**

Description

In Modem 2G RR, there is a possible out-of-bounds write due to missing bounds check. This could lead to remote code execution when decoding GPRS Packet Neighbour Cell

Data (PNCD) improper neighboring cell size with no additional execution privileges needed. User interaction is not needed for exploitation.

Improper authentication vulnerability in S&D Smarthome (CVE-2021-26638)

Severity: **MEDIUM**

Description

Improper Authentication vulnerability in S&D Smarthome(smartcare) application can cause authentication bypass and information exposure. Remote attackers can use this vulnerability to take control of the home environment including indoor control.

OS command injection vulnerability in Festo Controller CECC-X-M1 (CVE-2022-30308, CVE-2022-30309, CVE-2022-30310, CVE-2022-30311) Severity: **MEDIUM**

Description

In Festo Controller CECC-X-M1 product family in multiple versions, the http-endpoint "cecc-x-web-viewer-request-on" POST request doesn't check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.

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.