CERT Tonga

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

TLP: White[1]

Security Bulletin – June 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

OS Command injection vulnerability in Mintzo Docker-Tester (CVE-2021-34079*)* Severity: **HIGH**

Description

docker-tester is a Start a testing environment with a docker-compose file and verify it's up before running tests.

Affected versions of this package are vulnerable to Command Injection via shell meta-characters in the 'ports' entry of a crafted docker-compose.yml file.

How it works

Execution of malicious OS commands on the machine running docker-tester

What to do

Apply the appropriate updates as recommended Docker

Reference

https://advisory.checkmarx.net/advisory/CX-2021-4786/

OS Command Injection vulnerability in es128 ssl-utils (*CVE-2021-34080*, CVE-2021-34082, CVE-2021-34084*)* Severity: **HIGH**

Description

The ssl-utils package is a wrapper around OpenSSL commands for Node.js.

[1] CERT Tonga adopts the Traffic Light Protocol

How it works

The package is vulnerable to command injection. Exploitation is possible via unsanitized shell metacharacters provided to the createCertRequest() and the createCert() functions.

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://advisory.checkmarx.net/advisory/CX-2021-4782/

Remote code execution vulnerability in Tenda AC18 router V15.03.05.19 and V15.03.05.05 (*CVE-2022- 31446)* Severity: **HIGH**

Description

Tenda AC18 router V15.03.05.19 and V15.03.05.05 was discovered to contain a remote code execution (RCE) vulnerability via the Mac parameter at ip/goform/WriteFacMac.

How it works

The manipulation of the argument Mac with an unknown input led to a privilege escalation vulnerability.

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://github.com/wshidamowang/Router/blob/main/Tenda/AC18/RCE_1.md

Buffer Overflow vulnerability in Huawei CV81-WDM FW (*CVE-2022-29797)* Severity: **HIGH**

Description

Because of improper bounds checking, the Huawei CV81-WDM FW is vulnerable to buffer overflow.

How it works

A remote attacker might overflow a buffer and gain elevated access to the system by sending a carefully crafted request.

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220427-01-e9a493e2-en

Privilege escalation vulnerability in HID Mercury LP1501, LP1502, LP2500, LP4502 and EP4502 (*CVE-2022-31479)* Severity: **HIGH**

Description

An unauthenticated attacker can update the hostname with a specially crafted name that will allow for shell commands to be executed during the core collection process. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.302 for the LP series and 1.296 for the EP series

How it works

An attacker with this level of access on the device can monitor all communications sent to and from this device, modify onboard relays, change configuration files, or cause the device to become unstable. The injected commands only get executed during startup or when unsafe calls regarding the hostname are used. This allows the attacker to gain remote access to the device and can make their persistence permanent by modifying the filesystem.

What to do

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

Reference

https://www.corporate.carrier.com/product-security/advisories-resources/

Command injection vulnerability in Open SSL (*CVE-2022-1292)* Severity: **HIGH**

Description

The c_rehash script does not properly sanitize shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed.

How it works

On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. The use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command-line tool. The vulnerability is fixed in OpenSSL 3.0.3, OpenSSL 1.1.1o, and OpenSSL 1.0.2ze.

What to do

Make sure that you apply the appropriate updates recommended by Open SSL.

Reference

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=1ad73b4d27bd8c1b369a3cd453681d3a4f1bb9b2

Arbitrary code execution vulnerability in Aruba ClearPass Policy Manager (*CVE-2022-23657, CVE-2022-23658, CVE-2022-23660)* Severity: **HIGH**

Description

Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to run arbitrary commands on the underlying host.

How it works

Successful exploitation of these vulnerabilities allows an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.

What to do

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

Reference

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-007.txt

Command injection vulnerability in Thecus N4800Eco Nas Server Control Panel (*CVE-2021-34111)* Severity: **HIGH**

Description

Vulnerabilities found in Thecus Nas Sever Control Panel

How it works

Thecus 4800Eco was discovered to contain a command injection vulnerability via the username parameter in /adm/setmain.php.

What to do

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

Reference

https://docs.unsafe-inline.com/0day/thecus-n4800eco-nas-server-control-panel-comand-injection

Other Vulnerabilities with known Exploits

Stack-based overflow vulnerability in Fieldcomm Group HART-IP (CVE-2020-16209)

Severity: **MEDIUM**

Description

The HART-IP server component hipserver takes HART-IP messages from its clients and transports the embedded HART messages to various HART application programs. An unchecked memory transfer in the IP interface would potentially allow an internal buffer to overflow. A malicious user could exploit this interface by constructing HART-IP messages with payloads sufficiently large to overflow the internal buffer and crash the device or obtain control of the device.

Mali GPU Kernel Driver allows access to already freed memory (CVE-2022-28349, CVE-2022-28348) Severity: **MEDIUM**

Description

The vulnerability affects Valhall GPU Kernel Driver: All versions from r29p0 - r36p0. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This issue is fixed in Valhall GPU Kernel Driver r37p0.

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.