CERT Tonga

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

TLP: White[1]

Security Bulletin – February 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

Out-of-bounds Write vulnerability in Insyde Insydeh2O (*CVE-2021-42554)* Severity: **HIGH**

Description

An unauthenticated attacker could use the SMM memory corruption issue to write fixed or predictable data to SMRAM.

How it works

Exploiting this flaw could result in privileges being escalated to SMM.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://www.insyde.com/security-pledge/SA-2022012

Heap buffer overflow in Google Android 12.0 gki buffer.cc (*CVE-2021-39675)* Severity: **HIGH**

Description

In GKI_getbuf of gki_buffer.cc, there is a possible out of bounds write due to a heap buffer overflow

How it works

This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

What to do

[1] CERT Tonga adopts the Traffic Light Protocol

Apply the appropriate updates as recommended by Vendor

Reference

https://source.android.com/security/bulletin/2022-02-01

DoS exec code bypass vulnerability in the Cisco Small Business RV345 (*CVE-2021-42311 & CVE-2021-42313)* Severity: **HIGH**

Description

The vulnerability is introduced when processing specific HTTP requests due to insufficient boundary checks. By sending malicious HTTP queries to a susceptible SSL VPN Gateway device, a threat actor could exploit this issue.

How it works

On successful exploitation, the attacker might get root access to the target device and execute code remotely.

What to do

Make sure that you apply the appropriate updates recommended by Cisco

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D

DoS exec code bypass vulnerability in the Cisco Small Business RV345 (*CVE-2022-20700, CVE-2022-20701, CVE-2022-20700)* Severity: **HIGH**

Description

Because of insufficient authorization enforcement mechanisms, the flaws can be triggered by submitting specific commands to an affected device. The vulnerability affects Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers

How it works

An attacker could do any of the following if successful:

- Execute arbitrary code
- Elevate privileges
- Execute arbitrary commands
- Bypass authentication and authorization protections
- Fetch and run unsigned software
- Cause denial of service (DoS)

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D

Other Vulnerabilities with known Exploits

Command Injection vulnerability in Totolink X5000R Firmware 9.1.0U.6118B20201102 (*CVE-2021-45733, 2021-45738, 2021-45742)* Severity: **MEDIUM**

Description: The function NTPSyncWithHost in TOTOLINK X5000R v9.1.0u.6118 B20201102 was discovered to have a command injection vulnerability. This vulnerability allows attackers to run arbitrary commands via the parameter host_time.

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.