TLP: White[1]

Security Bulletin – August 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

Buffer overflow vulnerability in the Realtek AP-Router SDK (CVE-2022-27255) Severity: **HIGH**

Description

In Realtek eCos RSDK 1.5.7p1 and MSDK 4.9.4p1, the SIP ALG function that rewrites SDP data has a stack-based buffer overflow.

How it works

This allows an attacker to remotely execute code without authentication via a crafted SIP packet that contains malicious SDP data.

What to do

Apply the appropriate updates as recommended by Realtek

Reference

https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2022-27255.pdf

Out of bound write vulnerability in Google Android 10.0/11.0/12.0 (CVE-2022-20229)

Severity**: HIGH**

Description

In bta_hf_client_handle_cind_list_item of bta_hf_client_at.cc, there is a possible out of bounds write due to a missing bounds check

1 CERT Tonga adopts the Traffic Light Protocol

How it works

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

What to do

Make sure that you apply the appropriate updates recommended by Google Android.

Reference

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

SQL injection vulnerability in Library Management System v1.0 (*CVE-2022-36728)* Severity: **HIGH**

Description

Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the RollNo parameter at /staff/delstu.php.

What to do

Dell recommends users to upgrade at the earliest opportunity.

Reference

https://github.com/k0xx11/bug_report/blob/main/vendors/kingbhob02/library-management-system/SQLi-17.md

Heap-based Buffer Overflow vulnerability in SINEMA Remote Connect Server (SRCS) VPN (CVE-2022-34819*)* Severity: **HIGH**

SIEMENS

Description

A vulnerability found in Sinema Remote Connect Server

How it works

SINEMA Remote Connect allows end users to remotely access plants and machines and leverages VPN connections between the control center, service engineers and installed plants, according to Siemens. The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device.

What to do

Siemens has released an update for several products and recommends updating to the latest version.

Reference

https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf

Memory corruption vulnerability in Google Android kernel (CVE-2022-20238) Severity: **HIGH**

Description

An issue was discovered in Google Android Kernel.

How it works

remap_pfn_range here may map out of size kernel memory (for example, may map the kernel area), and because the vma->vm_page_prot can also be controlled by userspace, so userspace may map the kernel area to be writable, which is easy to be exploited.

What to do

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

Reference

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

Command Injection vulnerability in Siemens products (CVE-2022-34820, CVE-2022-34821) Severity: **HIGH**

Description

SIEMENS

The application does not correctly escape some user provided fields during the authentication process.

How it works

This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges.

What to do

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

Reference

https://cert-portal.siemens.com/productcert/pdf/ssa-517377.pdf

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