TLP: White[1]

Security Bulletin – January 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

Privilege escalation vulnerability in Google Android TV *(CVE-2021-0889)* Severity: **HIGH**

Description

In Android TV, there is a possible silent pairing due to lack of rate limiting in the pairing flow.

How it works

This could lead to remote code execution with no additional execution privileges needed.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://source.android.com/security/bulletin/2021-11-01

Privilege escalation vulnerability in Google Android (*CVE-2021-0956)* Severity: **HIGH**

Description

There is a potential out of bounds write in NfcTag::discoverTechnologies (activation) in NfcTag.cpp due to an erroneous bounds check.

How it works

This could lead to remote privilege escalation without the need for additional System execution privileges.

1 CERT Tonga adopts the Traffic Light Protocol

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://source.android.com/security/bulletin/2021-12-01

Privilege escalation vulnerability in Auerswald COMpact (*CVE-2021-40859)* Severity: **HIGH**

Description

Backdoors were discovered in Auerswald COMpact 5500R 7.8A and 8.0B devices.

How it works

that allow attackers with access to the web-based management application full administrative access to the device.

What to do

Ensure that you apply the appropriate updates recommended by the vendor.

Reference

https://www.redteam-pentesting.de/en/advisories/rt-sa-2021-007/-auerswald-compact-multiple-backdoors

Arbitrary code execution vulnerability in OpenCATS 0.9.6 (*CVE-2021-41560)* Severity: **HIGH**

Description

Vulnerability found in OpenCATS through 0.9.6

How it works

It allows remote attackers to execute arbitrary code by uploading an executable file via lib/FileUtility.php.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://github.com/opencats/OpenCATS/commit/b1af3bde1f68bec1c703ad66a3e390f15ed8ebe1

https://github.com/Nickguitar/RevCAT

IoT Remote code execution vulnerability in Microsoft Defender (*CVE-2021-42311 & CVE-2021-42313)* Severity: **HIGH**

Description

Microsoft Defender for IoT Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-41365, CVE-2021-42310, CVE-2021-42313, CVE-2021-42314, CVE-2021-42315, CVE-2021-43882, CVE-2021-43889.

How it works

This vulnerability allows remote attackers to bypass authentication on Microsoft Azure Defender for IoT installations that are vulnerable.

What to do

Make sure that you apply the appropriate updates recommended by Microsoft

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42311

Remote code execution vulnerability in Microsoft Visual Studio (*CVE-2021-43907)* Severity: **HIGH**

Description

A remote attacker might use the Microsoft Visual Studio Code WSL Extension to execute arbitrary code on the system.

How it works

An attacker might use this vulnerability to execute arbitrary code on the system by delivering a specially crafted request.

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43907

Stack-based buffer overflow vulnerability in Garrett Metal Detectors (*CVE-2021-21903)* Severity: **HIGH**

Description

The CMA check udp crc function of Garrett Metal Detectors' iC Module CMA Version 5.0 contains a stack-based buffer overflow vulnerability. During a call to strcpy, a specially constructed packet can cause a stack-based buffer overflow.

How it works

An attacker can exploit this flaw by sending a malicious packet.

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://talosintelligence.com/vulnerability_reports/TALOS-2021-1355
https://garrett.com/security/walk-through/accessories

Privilege escalation vulnerability in UiPath Assistant 21.4.4 *(CVE-2021-44041)* Severity: **HIGH**

Description

UiPath Assistant 21.4.4 will load and execute attacker-controlled data from the file path supplied to the --dev-widget argument of the URI handler for uipath-assistant://.

How it works

This allows an attacker to execute code on a victim's machine or capture NTLM credentials by supplying a networked or WebDAV file path.

What to do

Vendor has released updated versions of the affected systems which address this issue.

Reference

https://docs.uipath.com/robot/docs/release-notes-2021-10-4

Authentication bypass vulnerability in Zoho ManageEngine Desktop Central and Desktop Central MSP (*CVE-2021-44515)* Severity: **HIGH**

Description

Zoho ManageEngine Desktop Central is vulnerable to authentication bypass.

How it works

This could lead to remote code execution on the server, as exploited in the wild in December 2021.

What to do

Make sure that you apply the appropriate updates recommended.

- For Enterprise builds 10.1.2127.17 and earlier, upgrade to 10.1.2127.18.
- For Enterprise builds 10.1.2128.0 through 10.1.2137.2, upgrade to 10.1.2137.3.
- For MSP builds 10.1.2127.17 and earlier, upgrade to 10.1.2127.18.

- For MSP builds 10.1.2128.0 through 10.1.2137.2, upgrade to 10.1.2137.3.

Reference

https://www.manageengine.com/products/desktop-central/cve-2021-44515-authentication-bypass-filter-configuration.html

Arbitrary code execution in Google Android versions *(CVE-2021-1049)* Severity: **HIGH**

Description

A malicious program can use this flaw to gain elevated access to the system.

How it works

A logic issue in the Unisoc slogmodem has resulted in the vulnerability. With higher privileges, a local program can run arbitrary code.

Affected Android versions: Android SoCAndroid ID: A-204256722

What to do

Make sure that you apply the appropriate updates recommended.

Reference

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

Remote code execution vulnerability in Microsoft Windows Security Center API *(CVE-2022-21874)* Severity: **HIGH**

Description

A remote attacker can use this flaw to execute arbitrary code on the victim system. The cause of this vulnerability is a flaw in the Windows Security Center API's input validation

How it works

A remote attacker can send a specially crafted request to the target system and execute arbitrary code.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21874

Remote code execution vulnerability in Microsoft DirectX Graphics Kernel *(CVE-2022-21898)*

Severity: **HIGH**

Description

The problem exists because of incorrect input validation.

How it works

An attacker can send a specially crafted request to the target system and have it executed arbitrary code. Successful exploitation will result in the entire compromise of the system

What to do

Make sure that you apply the appropriate updates recommended.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21898

Other Vulnerabilities with known Exploits

Remote code execution vulnerability in H2 database console (*CVE-2021-42392)* Severity: **MEDIUM**

Description: H2 is an open-source Java SQL database offering a lightweight in-memory solution that doesn't require data to be stored on a disk. Custom classes can be loaded from remote servers via JNDI in H2 Console versions 1.1.100 (2008-10-14) to 2.0.204 (2021-12-21). The H2 database's org.h2.util.JdbcUtils.get connection method takes the driver's class name and the database's URL as inputs. An attacker can cause remote code execution by passing a JNDI driver name and a URL to an LDAP or RMI server.

Other Vulnerabilities

SQL-injection vulnerability in Le-yan dental management system (*CVE-2022-22055)* Severity: **MEDIUM**

Description: Unauthenticated remote attackers can inject SQL instructions into the login page's input field to gain administrator privileges and perform arbitrary system operations or interrupt service.

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