CERT Tonga

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

**TLP: White**[1]

# Security Bulletin – April 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

**Remote Code Execution Vulnerability in Spring Cloud Functions** (*CVE-2022-22963)* Severity: **HIGH**

### Description

Spring Cloud Function is one of the features of Spring Cloud. It allows developers to write cloud-agnostic functions with Spring features.

### How it works

In Spring Cloud Function versions 3.1.6, 3.2.2, and older unsupported versions, when using routing functionality, it is possible for a user to provide a specially crafted SpEL as a routing expression that may result in remote code execution and access to local resources.

### What to do

Apply the appropriate updates as recommended by Vendor

### Reference

https://tanzu.vmware.com/security/cve-2022-22963

**Remote Code Execution Vulnerability in Spring Framework (Spring4Shell) (***CVE-2022-22963)* Severity: **HIGH**

### Description

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.

[1] CERT Tonga adopts the Traffic Light Protocol

### How it works

The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e., the default, it is not vulnerable to exploitation.

### What to do

Users of affected versions should upgrade to 3.1.7, 3.2.3. No other steps are necessary. Releases that have fixed this issue include:

Spring Cloud Function

- 3.1.7
- 3.2.3

### Reference

https://tanzu.vmware.com/security/cve-2022-22965

## **Buffer overflow vulnerability in ALLMediaServer 1.6** (*CVE-2022- 28381)* Severity: **HIGH**

### Description

Mediaserver.exe in ALLMediaServer 1.6 has a stack-based buffer overflow.

### How it works

This allows remote attackers to execute arbitrary code via a long string to TCP port 888.

### What to do

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

### Reference

https://github.com/Matrix07ksa/ALLMediaServer-1.6-Buffer-Overflow

## **SQL injection vulnerability in Pagekit** (*CVE-2021-44135)* Severity: **HIGH**

### Description

Pagekit/pagekit is a modular and lightweight CMS built with Symfony components and Vue.js. Affected versions of this package are vulnerable to SQL Injection via the configAction in SettingsController,

### How it works

This allows users to set the order of comments listing using ascending (ASC) and descending (DESC). That config then gets concatenated directly to the SQL query without sanitization.

### What to do

Ensure that you apply the most appropriate updates recommended.

### Reference

https://huntr.dev/bounties/82f09b08-ceeb-4249-8855-b8bc718c4868/

## **Out-of-bounds Read vulnerability in Qualcomm products** (*CVE-2021-35117)* Severity: **HIGH**

### Description

An Out of Bounds read may potentially occur while processing an IBSS beacon, in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IoT, Snapdragon Industrial IoT, Snapdragon Mobile, Snapdragon Voice & Music. This vulnerability affects an unknown part of the component IBSS Beacon Handler.

### How it works

Manipulation with an unknown input led to an information disclosure vulnerability.

### What to do

Make sure that you apply the most appropriate updates recommended by the Vendor

### Reference

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

## **Elevation of privilege vulnerability in eScan Anti-Virus** (*CVE-2021-26624)* Severity: **HIGH**

### Description

A local privilege escalation vulnerability due to a "runasroot" command in eScan Anti-Virus.

### How it works

This vulnerability is due to invalid arguments and insufficient execution conditions related to "runasroot" command. This vulnerability can induce remote attackers to exploit root privileges by manipulating parameter values.

### What to do

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

### Reference

https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=66596

**Risky cryptographic algorithms in Dell PowerScale OneFS** (*CVE-2022- 26854)* Severity: **HIGH**

### Description

Dell PowerScale OneFS, versions 8.2.x-9.2.x, contain risky cryptographic algorithms

### How it works

A remote unprivileged malicious attacker could potentially exploit this vulnerability, leading to full system access

### What to do

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

### Reference

https://www.dell.com/support/kbdoc/en-us/000197991/dell-emc-powerscale-onefs-security-update-for-multiple-component-vulnerabilities

**Stack overflow vulnerability in the SetSysTimeCfg() function** (CVE-2022-27022, CVE-2022-27016*)* Severity: **HIGH**

### Description

There is a stack overflow vulnerability in the SetSysTimeCfg() and SetStaticRouteCfg() function in the httpd service of Tenda AC9 V15.03.2.21_cn.

### How it works

The attacker can obtain a stable root shell through a constructed payload.

### What to do

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

### Reference

https://github.com/EPhaha/IOT_vuln/tree/main/Tenda/AC9/10

**Command injection vulnerability in Python mailcap Module OS** (CVE-2015-20107) Severity: **HIGH**

### Description

In Python (aka CPython) through 3.10.4, the mailcap module does not add escape characters into commands discovered in the system mailcap file.

### How it works

This may allow attackers to inject shell commands into applications that call mailcap.findmatch with untrusted input (if they lack validation of user-provided filenames or arguments)..

### What to do

Make sure that you apply the appropriate security update recommended by Vendor.

### Reference

https://bugs.python.org/issue24778

**WSO2 Unrestricted Arbitrary File Upload and Remote Code Execution Vulnerability** (CVE-2022-29464*)* Severity: **HIGH**

### Description

Certain WSO2 products allow unrestricted file upload with resultant remote code execution.

### How it works

The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0.

### What to do

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

### Reference

https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738

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.