CERT Tonga

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

TLP: Clear[1]

Security Bulletin – April 2023

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

A Vulnerability found in Canon imageCLASS MF644Cdw *(CVE-2022-24673)*

Severity: **CRITICAL**

Description

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Canon image CLASS MF644Cdw 10.02 printers.

How it works

Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the SLP protocol. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://www.usa.canon.com/support/canon-product-advisories/canon-laser-printer-inkjet-printer-and-small-office-multifunctional-printer-measure-against-buffer-overflow

[1] CERT Tonga adopts the Traffic Light Protocol

Vulnerability found in Apple (CVE-*2023-28206)* Severity: CRITICAL

Description

A use after free issue was addressed with improved memory management in Apple Products.

How it works

This issue is fixed in macOS Ventura 13.3.1, iOS 16.4.1 and iPadOS 16.4.1, iOS 15.7.5 and iPadOS 15.7.5, Safari 16.4.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

What to do

Ensure that you apply the appropriate updates recommended by Apple.

Reference

https://support.apple.com/en-us/HT213723
https://support.apple.com/en-us/HT213722
https://support.apple.com/en-us/HT213721
https://support.apple.com/en-us/HT213720

Vulnerability found in Sophos Web Application *(CVE-2023-1671)* Severity: CRITICAL

Description

Sophos Web Appliance older than version 4.3.10.4 is vulnerable.

How it works

This is due to pre-auth command injection allowing arbitrary code execution in the warn-proceed handler.

What to do

Sophos recommends that Sophos Web Appliance is protected by a firewall and not accessible via the public Internet.

Reference

https://www.sophos.com/en-us/security-advisories/sophos-sa-20230404-swa-rce

SQL Injection vulnerability found in Ming-Soft MCMS (*CVE-2020-20913)* Severity: CRITICAL

Description

SQL Injection vulnerability found in Ming-Soft MCMS v.4.7.2.

How it works

This allows a remote attacker to execute arbitrary code via basic_title parameter.

What to do

Apply the most appropriate updates recommended by vendor.

Reference

https://github.com/ming-soft/MCMS/issues/27

Windows Common Log File System Driver Elevation of Privilege Vulnerability (*CVE-2023-28252)* Severity: CRITICAL

Description

A privilege escalation vulnerability, an attacker with access to the system and enough ability to run code can successfully exploit to acquire SYSTEM privileges – the highest user privilege level in Windows.

How it works

The exploit allows for the alteration of the base log file in return forcing the system to treat a bogus element of the base log file as a real one.

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252

SAP Diagnostics Agent version 720 is vulnerable to code injection (*CVE-2023-27497)* Severity: CRITICAL

Description

SAP Diagnostics Agent version 720 is vulnerable to code injection.

How it works

This is allowing attackers to execute malicious scripts and compromise system confidentiality, integrity, and availability.

What to do

Apply the most appropriate updates recommended by vendor.

Reference

https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html

HAProxy versions 2.7.0 and 2.6.1 to 2.6.7 are vulnerable to HTTP request/response *(CVE-2023-25950)* Severity: CRITICAL

Description

HTTP request/response smuggling vulnerability in HAProxy version 2.7.0, and 2.6.1 to 2.6.7

How it works

It allows a remote attacker to alter a legitimate user's request. As a result, the attacker may obtain sensitive information or cause a denial-of-service (DoS) condition.

What to do

Apply the appropriate update for your system.

Reference

https://jvn.jp/en/jp/JVN38170084/
https://www.haproxy.org/

Vulnerability identified in Hikvision Hybrid *(CVE-2023-24482)* Severity: CRITICAL

Description

"Hikvision Hybrid SAN/Cluster Storage products are vulnerable to access control manipulation through crafted messages, enabling unauthorized admin access."

How it works

The attacker can exploit the vulnerability by sending crafted messages to the affected devices.

What to do

Hikvision has released a version to fix the vulnerability and Users can download patches/updates on the Hikvision official website.

Reference

https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-vulnerability-in-some-hikvision-hybrid-san-cluster-stor/

Android contains a use after free vulnerability in attribution_processor.cc *(CVE-2023-21096)* Severity: CRITICAL

Description

In OnWakelockReleased of attribution_processor.cc, there is a use after free that could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-254774758

How it works

As a result the attacker can execute a remote code execution without additional execution privileges.

What to do

Apply the appropriate updates recommended by the Vendor.

Reference

https://source.android.com/security/bulletin/2023-04-01

Vulnerability found in Zyxel ZyWall *(CVE-2023-28771)* Severity: CRITICAL

Description

Improper error message handling in some firewall versions

How it works

This could allow an unauthenticated attacker to execute some OS commands remotely by sending crafted packets to an affected device

What to do

Zyxel has released patches for an OS command injection vulnerability found by TRAPA Security and urges uses to install them for optimal protection.

Reference

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls

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 3.0

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.