TLP: Clear[1]

Security Bulletin – May 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 Zyxel *(CVE-2023-28769)* Severity: CRITICAL

Description

Multiple buffer overflow vulnerabilities were discovered in the web server of the affected.

How it works

devices Zyxel DX5401-B0 firmware versions prior to V5.17(ABYO.1). This could potentially allow a remote attacker to execute OS commands or cause DoS via a buffer overflow vulnerability in the library "libclinkc.so" of the web server "zhttpd.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities

Vulnerability found in Apache Superset (*CVE- 2023-27524)* Severity: CRITICAL

Description

Session Validation attacks in Apache Superset versions up to and including 2.0.1.

How it works

Installations that have not altered the default configured SECRET_KEY according to installation instructions allow for an attacker to authenticate and access unauthorized

1 CERT Tonga adopts the Traffic Light Protocol

resources. This does not affect Superset administrators who have changed the default value for SECRET_KEY config.

What to do

Ensure that you apply the appropriate updates recommended by Apache.

Reference

https://lists.apache.org/thread/n0ftx60sllf527j7g11kmt24wvof8xyk

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

Vulnerabilities found in multiple version of Aruba (*CVE-2023-22779, CVE-2023-22780, CVE-2023-22781, CVE-2023-22782, CVE-2023-22783, CVE-2023-22784, CVE-2023-22785, CVE-2023-22786)* Severity: **CRITICAL**

Description

There are buffer overflow vulnerabilities in multiple underlying services of Aruba.

How it works

This allows an unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities will result in the ability to execute arbitrary code as a privileged user on the underlying operating system.

What to do

Apply the most appropriate updates recommended by vendor.

Reference

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt

Improper Privilege Management vulnerability in SUSE Rancher (*CVE- 2023-22651)* Severity: **CRITICAL**

Description

SUSE Rancher is vulnerable to improper privilege management, allowing for privilege escalation due to a failure in the update logic of Rancher's admission Webhook.

How it works

A failure in the update logic of Rancher's admission Webhook may lead to the misconfiguration of the Webhook. This component enforces validation rules and security checks before resources are admitted into the Kubernetes cluster.

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://bugzilla.suse.com/show_bug.cgi?id=CVE-2023-22651
https://github.com/rancher/rancher/security/advisories/GHSA-6m9f-pj6w-w87g

An Arbitrary Command Execution vulnerability in the router's web server

(*CVE-2023-31587)* Severity: **CRITICAL**

Description

Tenda AC5 router V15.03.06.28 was discovered to contain a remote code execution (RCE) vulnerability via the Mac parameter at ip/goform/WriteFacMac.

How it works

Arbitrary Command Execution vulnerability in the router's web server-- /bin/httpd of squashfs filesystem. While processing the mac parameters for a post request(when an attacker accesses ip/goform/WriteFacMac), the value is directly passed to doSystem, which causes a RCE. The details are shown below:

What to do

Apply the most appropriate updates recommended by vendor.

Reference

https://fortiguard.com/psirt/FG-IR-23-013

Synology Router Manager (SRM) versions are vulnerable to OS command injection. *(CVE-2023-32956)* Severity: CRITICAL

Description

Multiple vulnerabilities allow remote attackers to execute arbitrary command, conduct denial-of-service attacks or read arbitrary files via a susceptible version of Synology Router Manager (SRM)

How it works

Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to execute arbitrary code via unspecified vectors.

What to do

Apply the most appropriate updates recommended by vendor.

Reference

https://www.synology.com/en-global/security/advisory/Synology_SA_22_25

A 'Cross-site Scripting' vulnerability in FortiNAC *(CVE-2023-22637)* Severity: CRITICAL

Description

FortiNAC is vulnerable to a Cross-site Scripting (XSS) flaw that could allow an attacker to remotely execute code via crafted licenses.

How it works

An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiNAC License Management would permit an authenticated attacker to trigger remote code execution via crafted licenses.

What to do

Apply the most appropriate updates recommended by vendor.

Reference

https://fortiguard.com/psirt/FG-IR-23-013

A vulnerability found in Open TSDB (*CVE-2023-25826)* Severity: CRITICAL

Description

Due to insufficient validation of parameters passed to the legacy HTTP query API, it is possible to inject crafted OS commands into multiple parameters and execute malicious code on the OpenTSDB host system.

How it works

This exploit exists due to an incomplete fix that was made when this vulnerability was previously disclosed as CVE-2020-35476. Regex validation that was implemented to restrict allowed input to the query API does not work as intended, allowing crafted commands to bypass validation.

What to do

Apply the appropriate update for your system.

Reference

https://github.com/OpenTSDB/opentsdb/pull/2275
https://www.synopsys.com/blogs/software-security/opentsdb/

A command injection vulnerability in TP-Link Archer (*CVE-2023-1389)* Severity: CRITICAL

Description

TP-Link Archer AX21 firmware versions prior to 1.1.4 Build 20230219 have a command injection vulnerability in the country form of the /cgi-bin/luci;stok=/locale endpoint.

How it works

The vulnerability could allow an attacker to run commands as root.

What to do

TP Link has released a version to fix the vulnerability. Apply the appropriate updates recommended by the Vendor.

Reference

https://www.tenable.com/security/research/tra-2023-11

A flaw has been identified in SAP Netweaver Application Server For Java (*CVE-2023-30744)* Severity: **CRITICAL**

Description

A vulnerability found in SAP AS NetWeaver JAVA versions SERVERCORE 7.50, J2EE-FRMW 7.50, and CORE-TOOLS 7.50.

How it works

An unauthenticated attacker can attach to an open interface and make use of an open naming and directory API to instantiate an object which has methods which can be called without further authorization and authentication.

What to do

Apply the appropriate updates recommended by the Vendor.

Reference

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

Vulnerability has been identified in Ruckus Wireless (*CVE-2023-25717 1)* Severity: **CRITICAL**

Description

Ruckus Wireless Admin suffers from several serious web application weaknesses.

How it works

It allows the attacker to execute remotely with Remote Code Execution (RCE), Server-Side Request Forgery (SSRF), Cross-Site Request Forgery (CSRF), and other conditions. This can result in total compromise of the affected devices.

What to do

Apply the appropriate updates recommended by the Vendor.

Reference

https://support.ruckuswireless.com/security_bulletins/315
https://cybir.com/2023/cve/proof-of-concept-ruckus-wireless-admin-10-4-unauthenticated-remote-code-execution-csrf-ssrf/

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