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

TLP: White[1]

Security Bulletin – December 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

Vulnerability in Zimbra Collaboration *(CVE-2022- 40602)* Severity: **HIGH**

Description

A flaw in the Zyxel LTE3301-M209 firmware verisons prior to V1.00(ABLG.6)C0

How it works

This could allow a remote attacker to access the device using an improper pre-configured password if the remote administration feature has been enabled by an authenticated administrator.

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-pre-configured-password-vulnerability-of-lte3301-m209

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Airflow Pig Provider (*CVE-2022 40189)* Severity: **HIGH**

Description

Apache Airflow allows an attacker to control commands executed in the task execution context, without write access to DAG files.

1 CERT Tonga adopts the Traffic Light Protocol

How it works

This issue affects Pig Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Pig Provider is installed (Pig Provider 4.0.0 can only be installed for Airflow 2.3.0+).

What to do

Ensure that you apply the appropriate updates recommended. Note that you need to manually install the Pig Provider version 4.0.0 in order to get rid of the vulnerability on top of Airflow 2.3.0+ version.

Reference

https://lists.apache.org/thread/yxnfzfw2w9pj5s785k3rlyly4y44sd15

OPTILINK OP-XT71000N V2.2 is vulnerable to Remote Code Execution (*CVE-2020-23583, CVE-2020-23584)* Severity: **HIGH**

Description

The issue occurs when the attacker sends an arbitrary code on "/diag_ping_admin.asp" to "PingTest". This upload arbitrary files through " /mgm_dev_upgrade.asp " which can "delete every file for Denial of Service.

How it works

An attacker can successfully trigger the COMMAND and can compromise full system. - Unauthenticated remote code execution in OPTILINK OP-XT71000N, Hardware Version: V2.2 occurs when the attacker passes arbitrary commands with IP-ADDRESS sing " | " to execute commands on " /diag_tracert_admin.asp " in the "PingTest" parameter that leads to command execution.

What to do

Make sure to apply the appropriate updates recommended by the Vendor.

Reference

https://github.com/huzaifahussain98

A CSS injection vulnerability in BBCode Plugin (*CVE-2022-46162)* Severity: **HIGH**

Description

Discourse-bbcode is the official BBCode plugin for Discourse.

How it works

Prior to commit 91478f5, CSS injection can occur when rendering content generated with the discourse-bccode plugin. This

vulnerability only affects sites which have the discourse-bbcode plugin installed and enabled. This issue is patched in commit 91478f5. As a workaround, ensure that the Content Security Policy is enabled and monitor any posts that contain bbcode.

What to do

Make sure that you apply the most appropriate updates recommended.

Reference

https://github.com/discourse/discourse-bbcode/commit/91478f5cfecdcc43cf85b997168a8ecfd0f8df90

A vulnerability in the Cisco Discovery Protocol on CISCO IP Phone(*CVE-2022-20968)*

Severity: **HIGH**

Description

A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware.

How it works

This could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U

VMware ESXi, Workstation, and Fusion contain a heap out-of-bounds write vulnerability (*CVE-2022 40189)* Severity: **HIGH**

Description

VMware ESXi, Workstation, and Fusion contain a heap out-of-bounds write vulnerability in the USB 2.0 controller (EHCI).

How it works

This issue affects Pig Provider versions prior to 4.0.0. It also impacts any Apache Airflow versions prior to 2.3.0 in case Pig Provider is installed (Pig Provider 4.0.0 can only be installed for Airflow 2.3.0+).

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://www.vmware.com/security/advisories/VMSA-2022-0033.html?is=1f1bdb77c51b48495e7f3caa27c5331c9c71b196d0daa350d641b364432a9b90

A vulnerability found in SAP NetWeaver (*CVE-2022-41271)* Severity: **HIGH**

Description

An unauthenticated user can attach to an open interface exposed through JNDI by the Messaging System of SAP NetWeaver Process Integration (PI) - version 7.50

How it works

This user can make use of an open naming and directory API to access services that could perform unauthorized operations. The vulnerability affects local users and data, leading to a considerable impact on confidentiality as well as availability and a limited impact on the integrity of the application. These operations can be used to: * Read any information * Modify sensitive information * Denial of Service attacks (DoS) * SQL Injection

What to do

Ensure that you apply the appropriate updates recommended.

Reference

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

A vulnerability was found in SourceCodester Canteen Management System (*CVE-2022-4222, CVE-2022-4229, CVE-2022-4232)* Severity: **HIGH**

Description A vulnerability was found in SourceCodester Canteen Management System. It has been rated as critical.

How it works

This issue affects the function query of the file ajax_invoice.php of the component POST Request Handler. The manipulation of the argument search leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-214523

What to do

Make sure to apply the appropriate updates recommended by the Vendor.

Reference

https://www.jianshu.com/p/bda61089bf1d

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