CERT Tonga

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

TLP: White[1]

Security Bulletin – January 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

Vulnerability found in Apache Dubbo *(CVE-2021-32824)* Severity: **HIGH**

Description

Apache Dubbo is a java based, open source RPC framework. Versions prior to 2.6.10 and 2.7.10 are vulnerable to pre-auth remote code execution via arbitrary bean manipulation in the Telnet handler.

How it works

The Dubbo main service port can be used to access a Telnet Handler which offers some basic methods to collect information about the providers and methods exposed by the service and it can even allow to shut down the service. This endpoint is unprotected. Additionally, a provider method can be invoked using the `invoke` handler. This handler uses a safe version of FastJson to process the call arguments. However, the resulting list is later processed with `PojoUtils.realize` which can be used to instantiate arbitrary classes and invoke its setters. Even though FastJson is properly protected with a default blocklist, `PojoUtils.realize` is not, and an attacker can leverage that to achieve remote code execution.

What to do

Apply the most appropriate updates as recommended by the Vendor

Reference

https://securitylab.github.com/advisories/GHSL-2021-034_043-apache-dubbo/

[1] CERT Tonga adopts the Traffic Light Protocol

Out-of-bounds write vulnerability in Remote Desktop Functionality in Synology VPN Plus Server (*CVE-2022-43931)* Severity: **HIGH**

Description

Out-of-bounds write vulnerability in Remote Desktop Functionality in Synology VPN Plus Server before 1.4.3-0534 and 1.4.4-0635

How it works

This allows remote attackers to execute arbitrary commands via unspecified vectors.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://www.synology.com/en-global/security/advisory/Synology_SA_22_26

A vulnerability in the web-based management interface of Cisco Products (*CVE-2023-20025)* Severity: **HIGH**

Description

A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers

How it works

remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device.

What to do

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

Reference

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5

Improper Authetication issue found in authentik(*CVE-2022-23555)* Severity: **HIGH**

Description

authentik is an open-source Identity Provider focused on flexibility and versatility. Versions prior to 2022.11.4 and

2022.10.4 are vulnerable to Improper Authentication. Token reuse in invitation URLs leads to access control bypass via the use of a different enrollment flow than in the one provided.

How it works

The vulnerability allows an attacker that knows different invitation flows names (e.g. `enrollment-invitation-test` and `enrollment-invitation-admin`) via either different invite links or via brute forcing to signup via a single invitation url for any valid invite link received (it can even be a url for a third flow as long as it's a valid invite) as the token used in the `Invitations` section of the Admin interface does NOT change when a different `enrollment flow` is selected via the interface and it is NOT bound to the selected flow, so it will be valid for any flow when used. This issue is patched in authentik 2022.11.4,2022.10.4 and 2022.12.0. Only configurations that use invitations and have multiple enrollment flows with invitation stages that grant different permissions are affected. The default configuration is not vulnerable, and neither are configurations with a single enrollment flow. As a workaround, fixed data can be added to invitations which can be checked in the flow to deny requests. Alternatively, an identifier with high entropy (like a UUID) can be used as flow slug, mitigating the attack vector by exponentially decreasing the possibility of discovering other flows.

What to do

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

Reference

https://github.com/goauthentik/authentik/security/advisories/GHSA-9qwp-jf7p-vr7h

Improper Access Control issue found in InHand Network InRouter 302(*CVE-2023-22600, CVE-2023-22601*) Severity: **HIGH**

Description

InHand Networks InRouter 302, prior to version IR302 V3.5.56, and InRouter 615, prior to version InRouter6XX-S-V2.3.0.r5542, contain vulnerability CWE-284: Improper Access Control.

How it works

They allow unauthenticated devices to subscribe to MQTT topics on the same network as the device manager. An unauthorized user who knows of an existing topic name could send and receive messages to and from that topic. This includes the ability to send GET/SET configuration commands, reboot commands, and push firmware updates.

What to do

Make sure to apply the appropriate updates recommended by the Vendor

Reference

https://www.cisa.gov/uscert/ics/advisories/icsa-23-012-03

An incorrect authorization vulnerability was identified in GitHub Enterprise Server (*CVE-2022-23739)* Severity: **HIGH**

Description

An incorrect authorization vulnerability was identified in GitHub Enterprise Server, allowing for escalation of privileges in GraphQL API requests from GitHub Apps.

How it works

This vulnerability allowed an app installed on an organization to gain access to and modify most organization-level resources that are not tied to a repository regardless of granted permissions, such as users and organization-wide projects. Resources associated with repositories were not impacted, such as repository file content, repository-specific projects, issues, or pull requests. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.7.1 and was fixed in versions 3.3.16, 3.4.11, 3.5.8, 3.6.4, 3.7.1. This vulnerability was reported via the GitHub Bug Bounty program.

What to do

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

Reference

https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.16
https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.11
https://docs.github.com/en/enterprise-server@3.5/admin/release-notes#3.5.8
https://docs.github.com/en/enterprise-server@3.6/admin/release-notes#3.6.4
https://docs.github.com/en/enterprise-server@3.7/admin/release-notes#3.7.1

Inconsistent Interpretation of HTTP Requests (*CVE-2022-36760)* Severity: **HIGH**

Description

Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server

How it works

allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

What to do

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

Reference

https://httpd.apache.org/security/vulnerabilities_24.html

Vulnerability in the Oracle Communications Application Server(*CVE-2023-21890)* Severity: **HIGH**

Description

Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server

How it works

allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

What to do

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

Reference

https://www.oracle.com/security-alerts/cpujan2023.html

Authentication bypass vulnerability in TP-Link SG 105PE (*CVE-2023-22303)* Severity: **HIGH**

Description

TP-Link SG105PE firmware prior to 'TL-SG105PE(UN) 1.0_1.0.0 Build 20221208' contains an authentication bypass vulnerability.

How it works

Under the certain conditions, an attacker may impersonate an administrator of the product. As a result, information may be obtained and/or the product's settings may be altered with the privilege of the administrator.

What to do

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

Reference

https://www.tp-link.com/en/business-networking/easy-smart-switch/tl-sg105pe/

https://www.tp-link.com/jp/support/download/tl-sg105pe/v1/#Firmware

A vulnerability found in Apple Products (*CVE- CVE-2022-42856)* Severity: **HIGH**

Description

A type of confusion issue was addressed with improved state handling. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.1.2.

How it works

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 against versions of iOS released before iOS 15.1.

What to do

Ensure that you apply the most appropriate updates as recommended by Apple.

Reference

https://support.apple.com/en-us/HT213597

Other Vulnerabilities with known Exploits

Vulnerability occurs in LiuOS (*CVE-2022-46179*) Severity: **MEDIUM**

Description

LiuOS is a small Python project meant to imitate the functions of a regular operating system. Version 0.1.0 and prior of LiuOS allow an attacker to set the GITHUB_ACTIONS environment variable to anything other than null or true and skip authentication checks. This issue is patched in the latest commit (c658b4f3e57258acf5f6207a90c2f2169698ae22) by requiring the var to be set to true, causing a test script to run instead of being able to login. A potential workaround is to check for the GITHUB_ACTIONS environment variable and set it to "" (no quotes) to null the variable and force credential checks.

Unauthenticated User to execute arbitrary code on the server (*CVE-2015-10060*) Severity: **MEDIUM**

Description

erohtar/Dasherr is a dashboard for self-hosted services. In affected versions unrestricted file upload allows any unauthenticated user to execute arbitrary code on the server. The file /www/include/filesave.php allows for any file to uploaded to anywhere. If an attacker uploads a php file they can execute code on the server. This issue has been addressed in version 1.05.00. Users are advised to upgrade. There are no known workarounds for this issue.

A vulnerability was found in MNBikeways database (*CVE-2015-10060*) Severity: **MEDIUM**

Description

A vulnerability was found in MNBikeways database and classified as critical. This issue affects some unknown processing of the file Data/views.py. The manipulation of the argument id1/id2 leads to sql injection. The name of the patch is 829a027aca7c17f5a7ec1addca8dd5d5542f86ac. It is recommended to apply a patch to fix this issue. The identifier VDB-218417 was assigned to this vulnerability.

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.