TLP: White[1]

Security Bulletin – September 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

Heap based buffer overflow vulnerability in WhatsApp (CVE-2022-36934*)* Severity: **HIGH**

Description

The vulnerability affects the unknown code of the component Video Call Handler.

How it works

An integer overflow in WhatsApp for Android prior to v2.22.16.12, Business for Android prior to v2.22.16.12, iOS prior to v2.22.16.12, Business for iOS prior to v2.22.16.12 could result in remote code execution in an established video call.

What to do

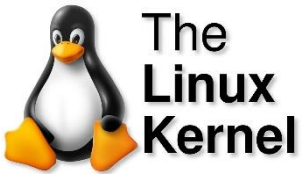
Apply the most appropriate updates as recommended by Whatsapp

Reference

https://www.whatsapp.com/security/advisories/2022/

Type Confusion vulnerability in the Linux Kernel (*CVE-2022-34918)* Severity: **HIGH**

Description



An issue was discovered in the Linux kernel through 5.18.9.

How it works

A type confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a local attacker to escalate privileges, a different vulnerability than CVE-2022-32250. (The attacker can obtain root access but must start with an unprivileged user

1 CERT Tonga adopts the Traffic Light Protocol

namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data in net/netfilter/nf_tables_api.c.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-d86f4869f452@randorisec.fr/T/#u

Use after poison vulnerability in MariaDB (*CVE-2022-32081)* Severity: **HIGH**

Description

Vulnerability found in MariaDB v10.4 to v10.7.

How it works

This was discovered to contain a use-after-poison in prepare_inplace_add_virtual at /storage/innobase/handler/handler0alter.cc.

What to do

Make sure to apply the appropriate updates recommended by Vendor

Reference

https://security.netapp.com/advisory/ntap-20220818-0005/

Cross-site Scripting (XSS) vulnerability in oauth2-server (CVE-2020-26938*)* Severity: **HIGH**

Description

In oauth2-server (aka node-oauth2-server) through 3.1.1, the value of the redirect_uri parameter received during the authorization and token request is checked against an incorrect URI pattern ("[a-zA-Z][a-zA-Z0-9+.-]+:") before making a redirection.

How it works

This allows a malicious client to pass an XSS payload through the redirect_uri parameter while making an authorization request. NOTE: This vulnerability is similar to CVE-2020-7741.

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

hhttps://github.com/oauthjs/node-oauth2-server/blob/91d2cbe70a0eddc53d72def96864e2de0fd41703/lib/grant-types/authorization-code-grant-type.js#L143

Heap-based buffer overwrite vulnerability in GhostScript package (*CVE-2020-27792)*

Severity: **HIGH**

Description

A heap-based buffer overwrite vulnerability was found in GhostScript's lp8000_print_page() function in gdevlp8k.c file.

How it works

An attacker could trick a user to open a crafted PDF file, triggering the heap buffer overflow that could lead to memory corruption or a denial of service.

What to do

Users are advised to upgrade. There are no known workarounds for this vulnerability.

Reference

https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=4f6bc662909ab79e8fbe9822afb36e8a0eafc2b7

Buffer over-read vulnerability in VRRP PARSER (CVE-2019-15167) Severity: **HIGH**

Description

The vulnerability affects the function vrrp_print of the file print-vrrp.c of the component VRRP Parser

How it works

The software reads from a buffer using buffer access mechanisms such as indexes or pointers that reference memory locations after the targeted buffer.

What to do

Please do ensure that you apply the most appropriate updates recommended.

Reference

https://sec-consult.com/vulnerability-lab/advisory/infiray-iray-thermal-camera-multiple-vulnerabilities/

Other Vulnerabilities with known Exploits

Out of bounds read vulnerability in libtar Tar File malloc gnu_longname (CVE-2021-33644, CVE-2021-33645) Severity: **MEDIUM**

Description

The vulnerability affects the malloc function of the Tar File Handler. An attacker who submits a crafted tar file with size in header struct being 0 may be able to trigger a calling of malloc(0) for a variable gnu_longname, causing an out-of-bounds read.

Out of bounds read vulnerability in libtar Tar File malloc (CVE-2021-33643, CVE-2021-33646) Severity: **MEDIUM**

Description

The vulnerability affects the malloc function of the Tar File Handler. An attacker who submits a crafted tar file with size in header struct being 0 may be able to trigger a calling of malloc(0) for a variable gnu_longlink, causing an out-of-bounds read.

Remote code execution vulnerability in Joblib (C CVE-2022-21797) Severity: **MEDIUM**

Description

The package joblib from 0 and before 1.2.0 are vulnerable to Arbitrary Code Execution via the pre_dispatch flag in Parallel() class due to the eval() statement.

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.