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

TLP: White[1]

Security Bulletin – May 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

Remote code execution vulnerability in VMware Workspace ONE Access and Identity Manager (*CVE-2022-22954)* Severity: **HIGH**

Description

VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability due to server-side template injection.

How it works

A malicious actor with network access can trigger a server-side template injection that may result in remote code execution.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://www.vmware.com/security/advisories/VMSA-2022-0011.html

Remote Code Execution Vulnerability in F5 BIG-IP iControl REST **(***CVE-2022-1388)*

Severity: **HIGH**

Description

On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication.

1 CERT Tonga adopts the Traffic Light Protocol

How it works

This vulnerability may allow an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands, create or delete files, or disable services.

What to do

Make sure that you apply the appropriate updates recommended by Vendor.

Reference

https://support.f5.com/csp/article/K23605346

Elevation of privilege vulnerability in Apache CouchDB (*CVE-2022- 24706)* Severity: **HIGH**

Description

A vulnerability found in Apache CouchDB prior to 3.2.2

How it works

In Apache CouchDB prior to 3.2.2, an attacker can access an improperly secured default installation without authenticating and gain admin privileges.

What to do

The CouchDB documentation has always made recommendations for properly securing an installation, including recommending using a firewall in front of all CouchDB installations.

Reference

https://lists.apache.org/thread/w24wo0h8nlctfps65txvk0oc5hdcnv00

Arbitrary command execution vulnerability in Terramaster (*CVE-2021-45837, CVE-2021-45840)* Severity: **HIGH**

Description

It is possible to execute arbitrary commands as root in Terramaster F4-210, F2-210 TOS 4.2.X (4.2.15-2107141517) by sending a specifically crafted input to /tos/index.php?app/del.

How it works

This allows root to access and execute commands in Terramaster

What to do

Ensure that you apply the most appropriate updates recommended.

Reference

https://thatsn0tmy.site/posts/2021/12/how-to-summon-rces/

Incorrection calculation vulnerability in Solana rBPF (*CVE-2022-23066)* Severity: **HIGH**

Description

In Solana rBPF versions 0.2.26 and 0.2.27 are affected by Incorrect Calculation which is caused by improper implementation of sdiv instruction.

How it works

This can lead to the wrong execution path, resulting in huge loss in specific cases. For example, the result of a sdiv instruction may decide whether to transfer tokens or not. The vulnerability affects both integrity and may cause serious availability problems.

What to do

Make sure that you apply the most appropriate updates recommended.

Reference

https://github.com/solana-labs/rbpf/commit/e61e045f8c244de978401d186dcfd50838817297
https://www.whitesourcesoftware.com/vulnerability-database/CVE-2022-23066

Improper authentication vulnerability in QNAP video station & photo (*CVE-2021-44056, CVE-2021-44057)* Severity: **HIGH**

Description

An improper authentication vulnerability has been reported to affect the QNAP device running Video and Photo Station

How it works

Successful exploitation of this vulnerability allows attackers to compromise the security of the system.

What to do

Make sure that you apply the appropriate updates recommended by QNAP.

Reference

https://www.qnap.com/en/security-advisory/qsa-22-14

Arbitrary command execution vulnerability in c_rehash scripts (*CVE-2022- 1292)* Severity: **HIGH**

Description

The c_rehash script does not properly sanitize shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed.

How it works

An attacker could execute arbitrary commands with the privileges of the script on such operating systems. The c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command-line tool

What to do

This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.

- OpenSSL 1.0.2 users should upgrade to 1.0.2ze (premium support customers only)
- OpenSSL 1.1.1 users should upgrade to 1.1.1o
- OpenSSL 3.0 users should upgrade to 3.0.3

Reference

https://www.openssl.org/news/secadv/20220503.txt

OS command injection vulnerability in Zyxel Firewall (CVE-2022-30525*)* Severity: **HIGH**

Description

Zyxel Communications Corp. is a manufacturer of DSL and other networking devices.

How it works

A command injection vulnerability in the CGI program of some firewall versions could allow an attacker to modify specific files and then execute some OS commands on a vulnerable device.

What to do

Make sure that you apply the appropriate updates recommended by Vendor.

Reference

https://www.zyxel.com/support/Zyxel-security-advisory-for-OS-command-injection-vulnerability-of-firewalls.shtml

Improper authentication vulnerability in SysAid wmiwizard.jsp (CVE-2015-22796)

Severity: **HIGH**

Description

A vulnerability found in Sysaid – Sysaid System.

How it works

An attacker can bypass the authentication process by accessing to: /wmiwizard.jsp, Then to: /ConcurrentLogin.jsp, then click on the login button, and it will redirect you to /home.jsp without any authentication.

What to do

Ensure that you apply the appropriate security update recommended by Vendor.

Reference

https://www.gov.il/en/departments/faq/cve_advisories

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.