CERT Tonga

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

TLP: White[1]

Security Bulletin – June 2021

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 vSphere Client *(CVE-2021-21985)* Severity: **HIGH**

Description

The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server.

How it works

A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server

What to do

Be sure to have the appropriate security updates recommended by vendor

Reference

https://www.vmware.com/security/advisories/VMSA-2021-0010.html

Weak Authentication Control in Python Version < 3,9,5 *(CVE-2021-29921)* Severity: **HIGH**

Description

In Python before 3,9,5, the ipaddress library mishandles leading zero characters in the octets of an IP address string.

[1] CERT Tonga adopts the Traffic Light Protocol

How it works

This (in some situations) allows attackers to bypass access control that is based on IP addresses.

What to do

Apply the most appropriate security update as recommended by the vendor.

Reference

https://bugs.python.org/issue36384

Weak Authorization Vulnerability in QNAP *(CVE-2021-28799)* Severity: **HIGH**

Description

An improper authorization vulnerability has been reported to affect QNAP NAS running HBS 3 (Hybrid Backup Sync.)

How it works

If exploited, the vulnerability allows remote attackers to log in to a device. This issue affects: QNAP Systems Inc. HBS 3 versions prior to v16.0.0415 on QTS 4.5.2; versions prior to v3.0.210412 on QTS 4.3.6; versions prior to v3.0.210411 on QTS 4.3.4; versions prior to v3.0.210411 on QTS 4.3.3; versions prior to v16.0.0419 on QuTS hero h4.5.1; versions prior to v16.0.0419 on QuTScloud c4.5.1~c4.5.4. This issue does not affect: QNAP Systems Inc. HBS 2. QNAP Systems Inc. HBS 1.3

What to do

To fix the vulnerability, we recommend updating HBS 3 to the latest version.

Reference

https://www.qnap.com/en/security-advisory/QSA-21-13

Arbitrary Code Execution Vulnerability in SolarWinds *(CVE-2021-31474)* Severity: **HIGH**

Description

This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Network Performance Monitor 2020.2.1. Authentication is not required to exploit this vulnerability

How it works

The specific flaw exists within the SolarWinds.Serialization library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM.

What to do

Ensure to apply the appropriate security updates recommended by vendor

Reference

https://documentation.solarwinds.com/en/success_center/sam/content/release_notes/sam_2020-2-5_release_notes.htm

Code Injection Vulnerability in SAP Solution Manager *(CVE-2020-6364)* Severity: **HIGH**

Description

Vulnerability found in SAP Solution Manager and SAP Focused Run (update provided in WILY_INTRO_ENTERPRISE 9.7, 10.1, 10.5, 10.7

How it works

It allows an attacker to modify a cookie in a way that OS commands can be executed and potentially gain control over the host running the CA Introscope Enterprise Manager,leading to Code Injection. With this, the attacker is able to read and modify all system files and also impact system availability.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://launchpad.support.sap.com/#/notes/2969828

SQL Injection Vulnerability in Synology Media Server *(CVE-2021-33180)*

Severity: **HIGH**

Description

Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in cgi component in Synology Media Server before 1.8.1-2876

How it works

It allows remote attackers to execute arbitrary SQL commands via unspecified vectors.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://www.synology.com/security/advisory/Synology_SA_20_24

Arbitrary Code Execution Vulnerability in SMbserver Instance *(CVE-2021-31800)* Severity: **HIGH**

Description

Multiple path traversal vulnerabilities exist in smbserver.py in Impacket through 0.9.22.

How it works

An attacker that connects to a running smbserver instance can list and write to arbitrary files via ../ directory traversal. This could potentially be abused to achieve arbitrary code execution by replacing /etc/shadow or an SSH authorized key.

What to do

Be sure to have the appropriate security updates recommended by vendor

Reference

https://github.com/SecureAuthCorp/impacket/commit/49c643bf66620646884ed141c94e5fdd85bcdd2f

Server Side Request Forgery Vulnerability in Apache Solr Core *(CVE-2021-27905)* Severity: **HIGH**

Description

A vulnerability found in Apache Solr Core

How it works

The ReplicationHandler (normally registered at "/replication" under a Solr core) in Apache Solr has a "masterUrl" (also "leaderUrl" alias) parameter that is used to designate another ReplicationHandler on another Solr core to replicate index data into the local core. To prevent a SSRF vulnerability, Solr ought to check these parameters against a similar configuration it uses for the "shards" parameter. Prior to this bug getting fixed, it did not.

What to do

This problem affects essentially all Solr versions prior to it getting fixed in 8.8.2.

Reference

https://lists.apache.org/thread.html/r0ddc3a82bd7523b1453cb7a5e09eb5559517145425074a42eb326b10%40%3Cannounce.apache.org%3E

Windows MSHTML Platform Remote Code Execution Vulnerability (*CVE-2021-33742)* Severity: **HIGH**

Description

This is a critical memory corruption vulnerability in the Chakra JScript scripting engine

How it works

This vulnerability impacts Windows RT, Windows 7, Windows 8, Windows 10, Windows Server 2008 R2, Windows Server 2012 (R2) and Windows Server 2016. An adversary can exploit this vulnerability when the target user opens a specially crafted file.

What to do

Be sure to appropriate security updates recommended by Microsoft

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742

Buffer Overflow Vulnerability in Oracle Solaris *(CVE-2020-14871)* Severity: **HIGH**

Description

Vulnerability in the Oracle Solaris product of Oracle Systems (component: Pluggable authentication module). Supported versions that are affected are 10 and 11.

How it works

Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Solaris.

While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris

What to do

Ensure that you apply the most appropriate updates that is recommended by Vendor

Reference

https://www.oracle.com/security-alerts/cpuoct2020.html

Weak Authentication Vulnerability in Apache Airflow *(CVE-2020-13927)* Severity: HIGH

Description

Authentication Vulnerability found in Apache Airflow.

How it works

The previous default setting for Airflow's Experimental API was to allow all API requests without authentication, but this poses security risks to users who miss this fact. From Airflow 1.10.11 the default has been changed to deny all requests by default and is documented at https://airflow.apache.org/docs/1.10.11/security.html#api-authentication.

What to do

Note this change fixes it for new installs but existing users need to change their config to default `[api]auth_backend = airflow.api.auth.backend.deny_all` as mentioned in the Updating Guide:
https://github.com/apache/airflow/blob/1.10.11/UPDATING.md#experimental-api-will-deny-all-request-by-default

Reference

https://lists.apache.org/thread.html/r23a81b247aa346ff193670be565b2b8ea4b17ddbc7a35fc099c1aadd%40%3Cdev.airflow.apache.org%3E

Deserialization Vulnerability in Apache Dubbo Server *(CVE-2021-25641)* Severity: HIGH

Description

Vulnerability found in Apache Dubbo server.

How it works

Each Apache Dubbo server will set a serialization id to tell the clients which serialization protocol it is working on. But for Dubbo versions before 2.7.8 or 2.6.9, an attacker can choose which serialization id the Provider will use by tampering with the byte preamble flags, aka, not following the server's instruction.

This means that if a weak deserializer such as the Kryo and FST are somehow in code scope (e.g. if Kryo is somehow a part of a dependency), a remote unauthenticated attacker can tell the Provider to use the weak deserializer, and then proceed to exploit it

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://lists.apache.org/thread.html/r99ef7fa35585d3a68762de07e8d2b2bc48b8fa669a03e8d84b9673f3%40%3Cdev.dubbo.apache.org%3E

Remote Code Execution Vulnerability in VoIP Monitor *(CVE-2021-30461)*

Severity: **HIGH**

Description

Remote Code Execution found in VoIP Monitor.

How it works

A remote code execution issue was discovered in the web UI of VoIPmonitor before 24.61. When the recheck option is used, the user-supplied SPOOLDIR value (which might contain PHP code) is injected into config/configuration.php.

What to do

Ensure to apply appropriate security updates recommended by vendor

Reference

https://ssd-disclosure.com/ssd-advisory--voipmonitor-unauth-rce

Other Vulnerabilities with known Exploits

Windows Kernel Information Disclosure Vulnerability (*CVE-2021-31955)* Severity: **MEDIUM**

Description: Description: This is an information disclosure vulnerability in ntoskrnl.exe. The vulnerability is affiliated with a Windows OS feature called SuperFetch. It was introduced in Windows Vista and is aimed to reduce software loading times by pre-loading commonly used applications into memory. For SuperFetch purposes the function NtQuerySystemInformation implements a special system information class SystemSuperfetchInformation. This system information class incorporates more than a dozen of different SuperFetch information classes. The vulnerability lies in the fact that data returned by the NtQuerySystemInformation function for the SuperFetch information class SuperfetchPrivSourceQuery contains EPROCESS kernel addresses for currently executed processes.

Memory Corruption Vulnerability in Gnutls *(CVE-2021-20231)* Severity: **MEDIUM**

Description: A flaw was found in gnutls. A use after free issue in client sending key_share extension may lead to memory corruption and other consequences.

Buffer Overflow Vulnerability in GNU *(CVE-2021-33574)* Severity: **MEDIUM**

Description: The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.

Denial of Service Vulnerability in GNU Screen (*CVE-2021-26937)* Severity: **MEDIUM**

Description: encoding.c in GNU Screen through 4.8.0 allows remote attackers to cause a denial of service (invalid write access and application crash) or possibly have unspecified other impact via a crafted UTF-8 character sequence.

Buffer Overflow Vulnerability in IcoFX (*CVE-2013-4988)* Severity: **MEDIUM**

Description: Stack-based buffer overflow in IcoFX 2.5 and earlier allows remote attackers to execute arbitrary code via a long idCount value in an ICONDIR structure in an ICO file. NOTE: some of these details are obtained from third party information.

Remote Code Execution Vulnerability in Microsoft Sharepoint (*CVE-2021-31950)* Severity: **MEDIUM**

Description: Description: Microsoft SharePoint Server Spoofing Vulnerability.

Code Injection Vulnerability in Smarty (*CVE-2021-26120)* Severity: **MEDIUM**

Description: Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.

Other Vulnerabilities

Authentication Bypass Vulnerability in Authelia (*CVE-2021-32637)* Severity: **MEDIUM**

Description: Authelia is a a single sign-on multi-factor portal for web apps. This affects uses who are using nginx ngx_http_auth_request_module with Authelia, it allows a malicious individual who crafts a malformed HTTP request to bypass the authentication mechanism. It additionally could theoretically affect other proxy servers, but all of the ones we officially support except nginx do not allow malformed URI paths. The problem is rectified entirely in v4.29.3. As this patch is relatively straightforward we can back port this to any version upon request. Alternatively we are supplying a git patch to 4.25.1 which should be relatively straightforward to apply to any version, the git patches for specific versions can be found in the references. The most relevant workaround is upgrading. You can also add a block which fails requests that contains a malformed URI in the internal location block.

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