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

TLP: White[1]

Security Bulletin – October 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

Buffer Overflow Vulnerability in QNap Device *(CVE-2021-34345)* Severity: HIGH

Description

A stack buffer overflow vulnerability has been reported to affect QNAP device running NVR Storage Expansion.

How it works

If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of NVR Storage Expansion: NVR Storage Expansion 1.0.6 (2021/08/03) and later.

What to do

To fix the vulnerabilities, it is recommended to update NVR Storage Expansion to the latest version.

Reference

qnap.com/en/security-advisory/qsa-21-36

Arbitrary Code Execution in Cisco Jabber *(CVE-2020-27134)* Severity: HIGH

Description

Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms.

[1] CERT Tonga adopts the Traffic Light Protocol

How it works

It could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information

What to do

Cisco has released software updates that address these vulnerabilities.

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-ZktzjpgO

Buffer Overflow Vulnerability in Aruba SD-WAN *(CVE-2021-37716)* Severity: **HIGH**

Description

There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of devices running ArubaOS

How it works

This may potentially allow for denial-of-service attacks and/or remote code execution in the underlying operating system

What to do

Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.

Reference

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt

Command injection Vulnerability in ssh2 *(CVE-2020-26301)* Severity: **HIGH**

Description

ssh2 is client and server modules written in pure JavaScript for node.js. In ssh2 before version 1.4.0 there is a command injection vulnerability.

How it works

The issue **only** exists on Windows. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. This is fixed in version 1.4.0.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://securitylab.github.com/advisories/GHSL-2020-123-mscdex-ssh2/

Denial of Service Vulnerability in Juniper Junos (*CVE-2021-2011)* Severity: **HIGH**

Description

An improper check for unusual or exceptional conditions in Juniper Networks Junos OS and Junos OS Evolved Routing Protocol Daemon (RPD) service.

‘How it works

It allows an attacker to send a valid BGP FlowSpec message thereby causing an unexpected change in the route advertisements within the BGP FlowSpec domain leading to disruptions in network traffic causing a Denial of Service (DoS) condition. Continued receipt of these update messages will cause a sustained Denial of Service condition.

This issue affects Juniper Networks: Junos OS: All versions prior to 17.3R3-S10 with the exceptions of 15.1X49-D240 on SRX Series and 15.1R7-S8 on EX Series; 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R2-S12, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R1-S3, 19.4R2-S3, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S3 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2. Junos OS Evolved: All versions prior to 20.3R1-S1-EVO, 20.3R2-EVO

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11062

Remote Code Execution Vulnerability in Genivia *(CVE-2021-21783)*

Severity: **HIGH**

Description

A code execution vulnerability exists in the WS-Addressing plugin functionality of Genivia gSOAP 2.8.107.

How it works

A specially crafted SOAP request can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://www.oracle.com/security-alerts/cpuoct2021.html

https://talosintelligence.com/vulnerability_reports/TALOS-2021-1245

XSS Vulnerability in Nodejs *(CVE-2021-22931)* Severity: **HIGH**

Description

Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to Remote Code Execution, XSS.

How it works

Application crashes due to missing input validation of host names returned by Domain Name Servers in Node.js dns library which can lead to output of wrong hostnames (leading to Domain Hijacking) and injection vulnerabilities in applications using the library.

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://nodejs.org/en/blog/vulnerability/aug-2021-security-releases/

Authentication Bypass Vulnerability in Dahua Products *(CVE-2021-33044)* Severity: HIGH

Description

The identity authentication bypass vulnerability found in some Dahua products during the login process.

How it works

Attackers can bypass device identity authentication by constructing malicious data packets.

What to do

Ensure to apply the most appropriate updates as recommended by the Vendor.

Reference

https://www.dahuasecurity.com/support/cybersecurity/details/957

Arbitrary Code Execution in PyYaml *CVE-2020-14343)* Severity: HIGH

Description

A vulnerability was discovered in the PyYAML library in versions before 5.4, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the full_load method or with the FullLoader loader. Applications that use the library to process untrusted input may be vulnerable to this flaw.

How it works

This flaw allows an attacker to execute arbitrary code on the system by abusing the python/object/new constructor**.** This flaw is due to an incomplete fix for CVE-2020-1747

What to do

Apply the appropriate updates as recommended by Vendor

Reference

https://bugzilla.redhat.com/show_bug.cgi?id=1860466

Weak Cryptography Usage in Mediawiki (*CVE-2021-31556)* Severity: **HIGH**

Description

An issue was discovered in the Oauth extension for MediaWiki through 1.35.2

How it works

MWOAuthConsumerSubmitControl.php does not ensure that the length of an RSA key will fit in a MySQL blob.

What to do

Ensure that you apply the appropriate updates recommended.

Reference

https://gerrit.wikimedia.org/r/c/mediawiki/extensions/OAuth/+/673566
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QNEAI2T3Y65I55ZB6UE6RMC662RZTGRX/

Other Vulnerabilities with known Exploits

SSRF Vulnerability in Apache Server (*CVE-2021-40438)* Severity: **MEDIUM**

Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

Win32K Elevation of Privilege Vulnerability (*CVE-2021-40449)* Severity: **MEDIUM**

Description: This is a use-after-free vulnerability in the NtGdiResetDC function of the Win32k driver. The vulnerability can lead to leakage of kernel module addresses in the computer’s memory. Cybercriminals then use the leak to elevate the privileges of another malicious process. Adversaries are deploying Trojans that begins by gathering information about the infected system and sends it to the C&C server. Then, through MysterySnail, the attackers can issue various commands. For example, they can create, read, or delete a specific file; create or delete a process; get a directory list; or open a proxy channel and send data through it. MysterySnail’s other features include the ability to view the list of connected drives, to monitor the connection of external drives in the background, and more. The Trojan can also launch the cmd.exe interactive shell (by copying the cmd.exe file to a temporary folder under a different name).

This vulnerability is being actively exploited by IronHusky and Chinese APT groups.

Improper Access Control in Emerson Devices (*CVE-2020-12030)* Severity: **MEDIUM**

Description: There is a flaw in the code used to configure the internal gateway firewall when the gateway's VLAN feature is enabled. If a user enables the VLAN setting, the internal gateway firewall becomes disabled resulting in exposure of all ports used by the gateway.

Apache HTTP Traversal Vulnerability (*CVE-2021-41773)* Severity: **MEDIUM**

Description: This vulnerability is in Apache Server version 2.4.49. It is a path traversal and file disclosure flaw that could allow attackers to gain access to sensitive data, and according to the report, is being actively exploited. This vulnerability allows attackers to map URLs to files outside of the expected document root using a path traversal attack. Path traversal attacks entail sending requests to get access to the backend or sensitive server directories that should not be accessible. The attackers bypass the filters using encoded characters (ASCII) for the URLs. According to the advisory, the problem might potentially reveal the source of interpreted files like CGI scripts, which could contain sensitive information that attackers could use for future attacks. The target must be running Apache HTTP Server 2.4.49 and have the “require all denied” access control parameter deactivated for the attack to work. However, this is the default setting.

Deserialization Vulnerability in Java xStream (*CVE-2021-21345)* Severity: **MEDIUM**

Description: XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker who has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.

Arbitrary File Read Vulnerability in Atlassian Confluence Server *(CVE-2021-26085)* Severity: **MEDIUM**

Description: Affected versions of Atlassian Confluence Server allow remote attackers to view restricted resources via a Pre-Authorization Arbitrary File Read vulnerability in the /s/ endpoint. The affected versions are before version 7.4.10, and from version 7.5.0 before 7.12.3

Other Vulnerabilities

Privilege Escalation Vulnerability in Flexera (*CVE-2020-12083)* Severity: **MEDIUM**

Description: An elevated privileges issue related to Spring MVC calls impacts Code Insight v7.x releases up to and including 2020 R1 (7.11.0-64).

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