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

TLP: White[1]

Security Bulletin – July 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

Deserialization Vulnerability in Spring Framework *(CVE-2020-5413)* Severity: **HIGH**

Description

Spring Integration framework provides Kryo Codec implementations as an alternative for Java (de)serialization.

How it works

When Kryo is configured with default options, all unregistered classes are resolved on demand. This leads to the "deserialization gadgets" exploit when provided data contains malicious code for execution during deserialization. In order to protect against this type of attack, Kryo can be configured to require a set of trusted classes for (de)serialization. Spring Integration should be proactive against blocking unknown "deserialization gadgets" when configuring Kryo in code

What to do

Users of an affected version should upgrade to these releases with the fixed issue:
Spring Integration

- 4.3.23
- 5.1.12
- 5.2.8
- 5.3.2

Reference

https://tanzu.vmware.com/security/cve-2020-5413

[1] CERT Tonga adopts the Traffic Light Protocol

Buffer Overflow Vulnerability in Ngnix Resolver *(CVE-2021-23017)* Severity: **HIGH**

Description

A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

How it works

This allows an attacker to cause 1-byte memory overwrite by using a specially crafted DNS response, resulting in worker process crash or, potentially, in arbitrary code execution.

What to do

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

Reference

http://mailman.nginx.org/pipermail/nginx-announce/2021/000300.html

Weak Authentication Vulnerability in Official Docker Compose *(CVE-2020-35184)* Severity: **HIGH**

Description

The official composer docker images before 1.8.3 contain a blank password for a root user.

How it works

System using the composer docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.

What to do

Apply the most appropriate updates as recommended by the Vendor.

Reference

https://github.com/koharin/koharin2/blob/main/CVE-2020-35184

Deserialization Vulnerability in Apache Log4j *(CVE-2017-5645)* Severity: HIGH

Description

A vulnerability found in Apache Log4j.

How it works

When using the TCP socket server or UDP socket server to receive serialized log events from another application, a specially crafted binary payload can be sent that, when deserialized, can execute arbitrary code

What to do

Apache Log4j 1.2 reached end of life in August 2015. Users should

upgrade to Log4j 2.x which both addresses that vulnerability as well

as numerous other issues in the previous versions.

Reference

https://issues.apache.org/jira/browse/LOG4J2-1863

Weak Authentication Vulnerability in SAP NetWeaver *(CVE-2020-26829)* Severity: HIGH

Description

SAP NetWeaver AS JAVA (P2P Cluster Communication), versions - 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows arbitrary connections from processes because of missing authentication check, that are outside the cluster and even outside the network segment dedicated for the internal cluster communication

How it works

An unauthenticated attacker can invoke certain functions that would otherwise be restricted to system administrators only, including access to system administration functions or shutting down the system completely.

What to do

Apply the appropriate security updates as recommended by the Vendor.

Reference

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564757079

Windows Print Spooler Remote Code Execution Vulnerability *(CVE-2021-34527)*

Severity: **HIGH**

Description

The Print Spooler remote code execution vulnerability takes advantage of the RpcAddPrinterDriver function call in the Print Spooler service that allows clients to add arbitrary dll files as printer drivers and load them as SYSTEM (the spooler service context).

How it works

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

What to do

Apply the most appropriate updates as recommended by the Microsoft.

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527

Weak Authentication Vulnerability in Dell EMC OpenManage *(CVE-2021-21513)* Severity: **HIGH**

Description

Dell EMC OpenManage Server Administrator (OMSA) version 9.5 Microsoft Windows installations with Distributed Web Server (DWS) enabled configuration contains an authentication bypass vulnerability

How it works

A remote unauthenticated attacker could potentially exploit this vulnerability to gain admin access on the affected system.

What to do

Install update from vendor's website as recommended.

Reference

https://www.dell.com/support/kbdoc/ru-ua/000183670/dsa-2021-040-dell-emc-openmanage-server-administrator-omsa-security-update-for-multiple-vulnerabilities

Windows Kernel Remote Code Execution Vulnerability *(CVE-2021-34458)* Severity: **HIGH**

Description

The vulnerability allows a remote attacker to execute arbitrary code on the target system. The vulnerability exists due to improper input validation in the Windows Kernel within the single root input/output virtualization (SR-IOV) device and Peripheral Component Interface Express (PCIe).

How it works

A remote authenticated attacker can send a specially crafted request and execute arbitrary code on the target system.

Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.

What to do

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

Reference

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34458

Denial of Service Vulnerability in Mozilla NSS (*CVE-2017-5461)* Severity: **HIGH**

Description

Mozilla Network Security Services (NSS) before 3.21.4, 3.22.x through 3.28.x before 3.28.4, 3.29.x before 3.29.5, and 3.30.x before 3.30.1

How it works

It allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by leveraging incorrect base64 operations.

What to do

Make sure to apply the appropriate security updates recommended by Mozilla

Reference

https://www.mozilla.org/en-US/security/advisories/mfsa2017-13/#CVE-2017-5461

Arbitrary Code Execution in XStream Library *(CVE-2021-21344)* Severity: **HIGH**

Description

An arbitrary code execution found in XStream Java library to serialize objects to XML and back again.

How it works

There is a vulnerability which may allow a remote attacker to load and execute arbitrary code from a remote 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.

What to do

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

Reference

http://x-stream.github.io/changes.html#1.4.16

Other Vulnerabilities with known Exploits

Code Injection Vulnerability in Dragonfly Gem (*CVE-2021-33564)* Severity: **MEDIUM**

Description: An argument injection vulnerability in the Dragonfly gem before 1.4.0 for Ruby allows remote attackers to read and write to arbitrary files via a crafted URL when the verify_url option is disabled. This may lead to code execution. The problem occurs because the generate and process features mishandle use of the ImageMagick convert utility.

Remote Code Execution Vulnerability in RebornCore Library *(CVE-2021-33790)* Severity: **MEDIUM**

Description: The RebornCore library before 4.7.3 allows remote code execution because it deserializes untrusted data in ObjectInputStream.readObject as part of reborncore.common.network.ExtendedPacketBuffer. An attacker can instantiate any class on the classpath with any data. A class usable for exploitation might or might not be present, depending on what Minecraft modifications are installed.

Improper Input Validation Vulnerability in Rocket Chat Server *(CVE-2021-22911)*

Severity: **MEDIUM**

Description: A improper input sanitization vulnerability exists in Rocket.Chat server 3.11, 3.12 & 3.13 that could lead to unauthenticated NoSQL injection, resulting potentially in RCE.

SQL Injection Vulnerability in WMS (*CVE-2020-18544)* Severity: **MEDIUM**

Description: SQL Injection in WMS v1.0 allows remote attackers to execute arbitrary code via the "username" parameter in the component "chkuser.php".

Other Vulnerabilities

Code Injection Vulnerability in Dragonfly Gem (*CVE-2021-33564)* Severity: **MEDIUM**

Description: An argument injection vulnerability in the Dragonfly gem before 1.4.0 for Ruby allows remote attackers to read and write to arbitrary files via a crafted URL when the verify_url option is disabled. This may lead to code execution. The problem occurs because the generate and process features mishandle use of the ImageMagick convert utility.

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