AppScan on Cloud

Security Report

Scan Name: SCA 2023-10-30 demo-sca.irx

Technology: SCA

Report Name: SCA-sample-security-report

Report created at: Monday, October 30, 2023

Notes: Sample security-report for SCA demo scan.

Summary of security issues

High severity issues:	7
Medium severity issues:	7
Total security issues:	**14**

Scan Information

Scan started: Monday, October 30, 2023 1:42:23 PM (UTC)

Table of Contents

How to Fix

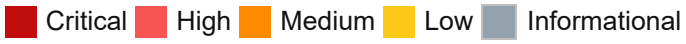
- Open Source Component

Summary

Total security issues: **14**

Issue Types: **1**

	Number of Issues
Open Source Component	14



Issues - By Fix Groups:

H	Common Open Source: Open Source Component: org.owasp.antisamy:antisamy
Fix Group ID:	b40f293b-2a77-ee11-826a-281878e63785
Status:	Open
Date:	2023-10-30 13:42:56Z
Library name:	org.owasp.antisamy:antisamy
Library Version:	1.5.8
Notes:	
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 4

Issue ID:	c00f293b-2a77-ee11-826a-281878e63785
Severity:	High
Status	Open
Fix Group ID:	b40f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/antisamy-1.5.8.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/antisamy-1.5.8.jar
CVSS	7.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2022-28366
CWE:	829

Issue 1 of 4 - Details

Name: **CVE-2022-28366**

Description: **Certain Neko-related HTML parsers allow a denial of service via crafted Processing Instruction (PI) input that causes excessive heap memory consumption. In particular, this issue exists in HtmlUnit-Neko through 2.26, and is fixed in 2.27. This issue also exists in CyberNeko HTML through 1.9.22 (also affecting OWASP AntiSamy before 1.6.6), but 1.9.22 is the last version of CyberNeko HTML. NOTE: this may be related to CVE-2022-24839.**

Resolution: **Upgrade package to version greater than or equal to 1.6.6**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-28366**

Issue 2 of 4

Issue ID:	ba0f293b-2a77-ee11-826a-281878e63785
Severity:	Medium
Status	Open
Fix Group ID:	b40f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/antisamy-1.5.8.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/antisamy-1.5.8.jar
CVSS	6.1
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2022-28367
CWE:	829

Issue 2 of 4 - Details

Name: **CVE-2022-28367**

Description: **OWASP AntiSamy before 1.6.6 allows XSS via HTML tag smuggling on STYLE content with crafted input. The output serializer does not properly encode the supposed Cascading Style Sheets (CSS) content.**

Resolution: **Upgrade package to version greater than or equal to 1.6.6**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-28367**

Issue 3 of 4

Issue ID:	b70f293b-2a77-ee11-826a-281878e63785
Severity:	Medium
Status	Open
Fix Group ID:	b40f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/antisamy-1.5.8.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/antisamy-1.5.8.jar
CVSS	6.1
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2021-35043
CWE:	829

Issue 3 of 4 - Details

Name: **CVE-2021-35043**

Description: **OWASP AntiSamy before 1.6.4 allows XSS via HTML attributes when using the HTML output serializer (XHTML is not affected). This was demonstrated by a javascript: URL with &#00058 as the replacement for the : character.**

Resolution: **Upgrade package to version greater than or equal to 1.6.4**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-35043**

Issue 4 of 4

Issue ID:	bd0f293b-2a77-ee11-826a-281878e63785
Severity:	**Medium**
Status	Open
Fix Group ID:	b40f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/antisamy-1.5.8.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/antisamy-1.5.8.jar
CVSS	6.1
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2022-29577
CWE:	829

Issue 4 of 4 - Details

Name: **CVE-2022-29577**

Description: **OWASP AntiSamy before 1.6.7 allows XSS via HTML tag smuggling on STYLE content with crafted input. The output serializer does not properly encode the supposed Cascading Style Sheets (CSS) content. NOTE: this issue exists because of an incomplete fix for CVE-2022-28367.**

Resolution: **Upgrade package to version greater than or equal to 1.6.7**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-29577**

H Common Open Source: Open Source Component: org.apache.commons:commons-compress

Fix Group ID:	af0f293b-2a77-ee11-826a-281878e63785
Status:	Open
Date:	2023-10-30 13:42:56Z
Library name:	org.apache.commons:commons-compress
Library Version:	1.2
Notes:	
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 6

Issue ID:	cf0f293b-2a77-ee11-826a-281878e63785
Severity:	High
Status	Open
Fix Group ID:	af0f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
CVSS	7.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2021-35516
CWE:	829

Issue 1 of 6 - Details

Name: **CVE-2021-35516**

Description: **When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.**

Resolution: **Upgrade package to version greater than or equal to 1.21**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-35516**

Issue 2 of 6

Issue ID:	cc0f293b-2a77-ee11-826a-281878e63785
Severity:	High
Status	Open
Fix Group ID:	af0f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
CVSS	7.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2021-35515
CWE:	829

Issue 2 of 6 - Details

Name: **CVE-2021-35515**

Description: **When reading a specially crafted 7Z archive, the construction of the list of codecs that decompress an entry can result in an infinite loop. This could be used to mount a denial of service attack against services that use Compress' sevenz package.**

Resolution: **Upgrade package to version greater than or equal to 1.21**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-35515**

Issue 3 of 6

Issue ID:	d50f293b-2a77-ee11-826a-281878e63785
Severity:	High
Status	Open
Fix Group ID:	af0f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
CVSS	7.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2021-36090
CWE:	829

Issue 3 of 6 - Details

Name: **CVE-2021-36090**

Description: **When reading a specially crafted ZIP archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' zip package.**

Resolution: **Upgrade package to version greater than or equal to 1.21**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-36090**

Issue 4 of 6

Issue ID:	d20f293b-2a77-ee11-826a-281878e63785
Severity:	High
Status	Open
Fix Group ID:	af0f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
CVSS	7.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2021-35517
CWE:	829

Issue 4 of 6 - Details

Name: **CVE-2021-35517**

Description: **When reading a specially crafted TAR archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' tar package.**

Resolution: **Upgrade package to version greater than or equal to 1.21**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-35517**

Issue 5 of 6

Issue ID:	c90f293b-2a77-ee11-826a-281878e63785
Severity:	Medium
Status	Open
Fix Group ID:	af0f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
CVSS	5.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2018-11771
CWE:	829

Issue 5 of 6 - Details

Name: **CVE-2018-11771**

Description: **When reading a specially crafted ZIP archive, the read method of Apache Commons Compress 1.7 to 1.17's ZipArchiveInputStream can fail to return the correct EOF indication after the end of the stream has been reached. When combined with a java.io.InputStreamReader this can lead to an infinite stream, which can be used to mount a denial of service attack against services that use Compress' zip package.**

Resolution: **Upgrade package to version greater than or equal to 1.18**

URL: **https://www.cve.org/CVERecord?id=CVE-2018-11771**

Issue 6 of 6

Issue ID:	d80f293b-2a77-ee11-826a-281878e63785
Severity:	Medium
Status	Open
Fix Group ID:	af0f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-compress-1.2.jar
CVSS	5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2012-2098
CWE:	829

Issue 6 of 6 - Details

Name: **CVE-2012-2098**

Description: Algorithmic complexity vulnerability in the sorting algorithms in bzip2 compressing stream (BZip2CompressorOutputStream) in Apache Commons Compress before 1.4.1 allows remote attackers to cause a denial of service (CPU consumption) via a file with many repeating inputs.

Resolution: Upgrade package to version greater than or equal to 1.4.1

URL: https://www.cve.org/CVERecord?id=CVE-2012-2098

M Common Open Source: Open Source Component: commons-io:commons-io

Fix Group ID:	b20f293b-2a77-ee11-826a-281878e63785
Status:	Open
Date:	2023-10-30 13:42:56Z
Library name:	commons-io:commons-io
Library Version:	2.1
Notes:	
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 1

Issue ID:	b50f293b-2a77-ee11-826a-281878e63785
Severity:	Medium
Status	Open
Fix Group ID:	b20f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-io-2.1.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/commons-io-2.1.jar
CVSS	4.8
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2021-29425
CWE:	829

Issue 1 of 1 - Details

Name: CVE-2021-29425

Description: In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "//../foo", or "\\..\foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.

Resolution: Upgrade package to version greater than or equal to 2.7

URL: https://www.cve.org/CVERecord?id=CVE-2021-29425

M Common Open Source: Open Source Component: com.fasterxml.jackson.datatype:jackson-datatype-jsr310

Fix Group ID:	b30f293b-2a77-ee11-826a-281878e63785
Status:	Open
Date:	2023-10-30 13:42:56Z
Library name:	com.fasterxml.jackson.datatype:jackson-datatype-jsr310
Library Version:	2.9.7
Notes:	
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 1

Issue ID:	c30f293b-2a77-ee11-826a-281878e63785
Severity:	Medium
Status	Open
Fix Group ID:	b30f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/jackson-datatype-jsr310-2.9.7.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/jackson-datatype-jsr310-2.9.7.jar
CVSS	6.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2018-1000873
CWE:	829

Issue 1 of 1 - Details

Name: **CVE-2018-1000873**

Description: **Fasterxml Jackson version Before 2.9.8 contains a CWE-20: Improper Input Validation vulnerability in Jackson-Modules-Java8 that can result in Causes a denial-of-service (DoS). This attack appear to be exploitable via The victim deserializes malicious input, specifically very large values in the nanoseconds field of a time value. This vulnerability appears to have been fixed in 2.9.8.**

Resolution: **Upgrade package to version greater than or equal to 2.9.8**

URL: **https://www.cve.org/CVERecord?id=CVE-2018-1000873**

H Common Open Source: Open Source Component: org.jdom:jdom

Fix Group ID:	b10f293b-2a77-ee11-826a-281878e63785
Status:	Open
Date:	2023-10-30 13:42:56Z
Library name:	org.jdom:jdom
Library Version:	1.1
Notes:	
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 1

Issue ID:	db0f293b-2a77-ee11-826a-281878e63785
Severity:	High
Status	Open
Fix Group ID:	b10f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/jdom-1.1.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/jdom-1.1.jar
CVSS	7.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2021-33813
CWE:	829

Issue 1 of 1 - Details

Name: **CVE-2021-33813**

Description: **An XXE issue in SAXBuilder in JDOM through 2.0.6 allows attackers to cause a denial of service via a crafted HTTP request.**

Resolution: **Upgrade package to version greater than 2.0.6**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-33813**

H Common Open Source: Open Source Component: net.minidev:json-smart

Fix Group ID:	b00f293b-2a77-ee11-826a-281878e63785
Status:	Open
Date:	2023-10-30 13:42:56Z
Library name:	net.minidev:json-smart
Library Version:	2.4.8
Notes:	
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 1

Issue ID:	c60f293b-2a77-ee11-826a-281878e63785
Severity:	High
Status	Open
Fix Group ID:	b00f293b-2a77-ee11-826a-281878e63785
Location	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/json-smart-2.4.8.jar
Source File	D:/StagingLatest/SCA_Testing/Java/LibraryJava/lib/json-smart-2.4.8.jar
CVSS	7.5
Date Created	Monday, October 30, 2023
Last Updated	Monday, October 30, 2023
CVE	https://www.cve.org/CVERecord?id=CVE-2023-1370
CWE:	829

Issue 1 of 1 - Details

Name: **CVE-2023-1370**

Description: **[Json-smart](https://netplex.github.io/json-smart/) is a performance focused, JSON processor lib. When reaching a '[' or '{' character in the JSON input, the code parses an array or an object respectively. It was discovered that the code does not have any limit to the nesting of such arrays or objects. Since the parsing of nested arrays and objects is done recursively, nesting too many of them can cause a stack exhaustion (stack overflow) and crash the software.**

Resolution: **Upgrade package to version greater than 2.4.9**

URL: **https://www.cve.org/CVERecord?id=CVE-2023-1370**

How to Fix

H Open Source Component

Cause

A vulnerable version of third party software component is installed in the tested application.

Risk

A vulnerable third party software component may introduce all manner of vulnerabilities into the application

Fix recommendation

Upgrade to the latest version of the third party software component. We highly recommend contacting the vendor of this product to see if a patch or fix has recently been made available.

CWE

829

External references

- CERT coordination center
- Common Vulnerabilities and Exposures (CVE)

Go to Table of Contents