AppScan 360°

HCL AppScan Report

Report Type: Security Report

Scan Name: Sample Report [demo.irx]

Technology: SCA

Report created at: Wednesday, July 16, 2025

This report was generated by HCL AppScan

Summary of security issues

Critical severity issues:	5
High severity issues:	19
Medium severity issues:	10
Low severity issues:	1
Total security issues: 35	

Scan Information

Scan started: Thursday, February 13, 2025 11:53:11 AM (UTC)

Method: Source code and config scanning

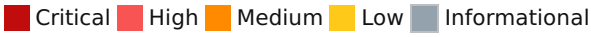
Table of Contents

Summary

Total security issues: **35**

Issue Types: **1**

	Number of Issues
Open Source Component	35



Issues - By Fix Groups:

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

Fix Group ID:	923f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:07Z
Library name:	org.apache.commons:commons-compress
Library Version:	1.19
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 5

Issue ID:	e23f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	923f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-compress-1.19.jar
Line	0
Source File	java_1/lib/commons-compress-1.19.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 5 - 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**

Dependency Root:

Issue 2 of 5

Issue ID:	c23f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	923f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-compress-1.19.jar
Line	0
Source File	java_1/lib/commons-compress-1.19.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 5 - 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

Dependency Root:

Issue 3 of 5

Issue ID:	d63f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	923f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-compress-1.19.jar
Line	0
Source File	java_1/lib/commons-compress-1.19.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 3 of 5 - 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

Dependency Root:

Issue 4 of 5

Issue ID:	d03f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	923f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-compress-1.19.jar
Line	0
Source File	java_1/lib/commons-compress-1.19.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 4 of 5 - 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

Dependency Root:

Issue 5 of 5

Issue ID:	fa3f443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Fix Group ID:	923f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-compress-1.19.jar
Line	0
Source File	java_1/lib/commons-compress-1.19.jar
CVSS	5.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 5 of 5 - Details

Name: **CVE-2024-25710**

Description: **Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Apache Commons Compress.This issue affects Apache Commons Compress: from 1.3 through 1.25.0.**

Users are recommended to upgrade to version 1.26.0 which fixes the issue.

Resolution: **Upgrade package to version greater than or equal to 1.26.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2024-25710**

Dependency Root:

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

Fix Group ID:	8f3f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	commons-httpclient:commons-httpclient
Library Version:	3.1
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 1

Issue ID:	c43f443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Fix Group ID:	8f3f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-httpclient-3.1.jar
Line	0
Source File	java_1/lib/commons-httpclient-3.1.jar
CVSS	5.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 1 - Details

Name: **CVE-2012-5783**

Description: **Apache Commons HttpClient 3.x, as used in Amazon Flexible Payments Service (FPS) merchant Java SDK and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.**

Resolution: **Upgrade package to version greater than or equal to 4.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2012-5783**

Dependency Root:

H	Common Open Source: Open Source Component: commons-io:commons-io
Fix Group ID:	b63f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	commons-io:commons-io
Library Version:	2.1
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 2

Issue ID:	e83f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	b63f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-io-2.1.jar
Line	0
Source File	java_1/lib/commons-io-2.1.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 2 - Details

Name: **CVE-2024-47554**

Description: **Apache Commons IO: Possible denial of service attack on untrusted input to XmlStreamReader**

Resolution: **Upgrade package to version greater than or equal to 2.14.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2024-47554**

Dependency Root:

Issue 2 of 2

Issue ID:	cc3f443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Fix Group ID:	b63f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-io-2.1.jar
Line	0
Source File	java_1/lib/commons-io-2.1.jar
CVSS	4.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 2 - 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**
Dependency Root:	

H	Common Open Source: Open Source Component: commons-io:commons-io
Fix Group ID:	a43f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	commons-io:commons-io
Library Version:	2.1
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 2

Issue ID:	f63f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	a43f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/commons-io-2.1.jar
Line	0
Source File	java_2/lib/commons-io-2.1.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 2 - Details

Name:	**CVE-2024-47554**
Description:	**Apache Commons IO: Possible denial of service attack on untrusted input to XmlStreamReader**
Resolution:	**Upgrade package to version greater than or equal to 2.14.0**
URL:	**https://www.cve.org/CVERecord?id=CVE-2024-47554**
Dependency Root:	

Issue 2 of 2

Issue ID:	f83f443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Fix Group ID:	a43f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/commons-io-2.1.jar
Line	0
Source File	java_2/lib/commons-io-2.1.jar
CVSS	4.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 2 - 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**
Dependency Root:	

H	Common Open Source: Open Source Component: commons-io:commons-io
Fix Group ID:	953f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	commons-io:commons-io
Library Version:	2.2
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 2

Issue ID:	e63f443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Fix Group ID:	953f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-io-2.2.jar
Line	0
Source File	java_1/lib/commons-io-2.2.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 2 - Details

Name:	**CVE-2024-47554**
Description:	**Apache Commons IO: Possible denial of service attack on untrusted input to XmlStreamReader**
Resolution:	**Upgrade package to version greater than or equal to 2.14.0**
URL:	**https://www.cve.org/CVERecord?id=CVE-2024-47554**
Dependency Root:	

Issue 2 of 2

Issue ID:	f43f443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Fix Group ID:	953f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/commons-io-2.2.jar
Line	0
Source File	java_1/lib/commons-io-2.2.jar
CVSS	4.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 2 - 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**
Dependency Root:	

H	Common Open Source: Open Source Component: commons-io:commons-io
Fix Group ID:	b03f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	commons-io:commons-io
Library Version:	2.2
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 2

Issue ID:	ce3f443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Fix Group ID:	b03f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/commons-io-2.2.jar
Line	0
Source File	java_2/lib/commons-io-2.2.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 2 - Details

Name:	**CVE-2024-47554**
Description:	**Apache Commons IO: Possible denial of service attack on untrusted input to XmlStreamReader**
Resolution:	**Upgrade package to version greater than or equal to 2.14.0**
URL:	**https://www.cve.org/CVERecord?id=CVE-2024-47554**
Dependency Root:	

Issue 2 of 2

Issue ID:	d23f443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Fix Group ID:	b03f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/commons-io-2.2.jar
Line	0
Source File	java_2/lib/commons-io-2.2.jar
CVSS	4.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 2 - 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**
Dependency Root:	

M	Common Open Source: Open Source Component: jackc/pgproto3/v2
Fix Group ID:	aa3f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	jackc/pgproto3/v2
Library Version:	v2.0.4
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 1

Issue ID:	d83f443e-f36b-1410-81f1-00524afcd01d
Severity:	**Medium**
Status	Open
Fix Group ID:	aa3f443e-f36b-1410-81f1-00524afcd01d
Location	go-part5/go.mod
Line	0
Source File	go-part5/go.mod
CVSS	0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 1 - Details

Name:	**CVE-2024-27304**
Description:	**pgx SQL Injection via Protocol Message Size Overflow**
Resolution:	**Upgrade package to version greater than or equal to 2.3.3**
URL:	**https://www.cve.org/CVERecord?id=CVE-2024-27304**
Dependency Root:	

M	Common Open Source: Open Source Component: jackc/pgx/v4
Fix Group ID:	983f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	jackc/pgx/v4
Library Version:	v4.8.1
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 2

Issue ID:	e03f443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Fix Group ID:	983f443e-f36b-1410-81f1-00524afcd01d
Location	go-part5/go.mod
Line	0
Source File	go-part5/go.mod
CVSS	0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 2 - Details

Name: **CVE-2024-27289**
Description: **pgx SQL Injection via Line Comment Creation**
Resolution: **Upgrade package to version greater than or equal to 4.18.2**
URL: **https://www.cve.org/CVERecord?id=CVE-2024-27289**
Dependency Root:

Issue 2 of 2

Issue ID:	f03f443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Fix Group ID:	983f443e-f36b-1410-81f1-00524afcd01d
Location	go-part5/go.mod
Line	0
Source File	go-part5/go.mod
CVSS	0
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 2 - Details

Name: **CVE-2024-27304**
Description: **pgx SQL Injection via Protocol Message Size Overflow**
Resolution: **Upgrade package to version greater than or equal to 4.18.2**
URL: **https://www.cve.org/CVERecord?id=CVE-2024-27304**
Dependency Root:

H	Common Open Source: Open Source Component: golang.org/x/text
Fix Group ID:	b33f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	golang.org/x/text
Library Version:	v0.3.3
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 2

Issue ID:	ba3f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	b33f443e-f36b-1410-81f1-00524afcd01d
Location	go-part5/go.mod
Line	0
Source File	go-part5/go.mod
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 2 - Details

Name:	**CVE-2022-32149**
Description:	**An attacker may cause a denial of service by crafting an Accept-Language header which ParseAcceptLanguage will take significant time to parse.**
Resolution:	**Upgrade package to version greater than or equal to 0.3.8**
URL:	**https://www.cve.org/CVERecord?id=CVE-2022-32149**
Dependency Root:	**github.com/jackc/pgconn v1.6.4**

Issue 2 of 2

Issue ID:	c63f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	b33f443e-f36b-1410-81f1-00524afcd01d
Location	go-part5/go.mod
Line	0
Source File	go-part5/go.mod
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 2 - Details

Name:	**CVE-2021-38561**
Description:	**golang.org/x/text/language in golang.org/x/text before 0.3.7 can panic with an out-of-bounds read during BCP 47 language tag parsing. Index calculation is mishandled. If parsing untrusted user input, this can be used as a vector for a denial-of-service attack.**
Resolution:	**Upgrade package to version greater than or equal to 0.3.7**
URL:	**https://www.cve.org/CVERecord?id=CVE-2021-38561**
Dependency Root:	**github.com/jackc/pgconn v1.6.4**

C	Common Open Source: Open Source Component: log4j:log4j
Fix Group ID:	9b3f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	log4j:log4j
Library Version:	1.2.16
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 6

Issue ID:	c03f443e-f36b-1410-81f1-00524afcd01d
Severity:	**Critical**
Status	Open
Fix Group ID:	9b3f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/log4j-1.2.16.jar
Line	0
Source File	java_2/lib/log4j-1.2.16.jar
CVSS	9.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 6 - Details

Name: **CVE-2022-23305**

Description: **By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unintended SQL queries to be executed. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default. Beginning in version 2.0-beta8, the JDBCAppender was re-introduced with proper support for parameterized SQL queries and further customization over the columns written to in logs. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.**

Resolution: **Upgrade package to version greater than 1.2.17**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-23305**

Dependency Root:

Issue 2 of 6

Issue ID:	b83f443e-f36b-1410-81f1-00524afcd01d
Severity:	**Critical**
Status	Open
Fix Group ID:	9b3f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/log4j-1.2.16.jar
Line	0
Source File	java_2/lib/log4j-1.2.16.jar
CVSS	9.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 6 - Details

Name: **CVE-2019-17571**

Description: **Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.**

Resolution: **Upgrade package to version greater than 1.2.27**

URL: **https://www.cve.org/CVERecord?id=CVE-2019-17571**

Dependency Root:

Issue 3 of 6

Issue ID:	ee3f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	9b3f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/log4j-1.2.16.jar
Line	0
Source File	java_2/lib/log4j-1.2.16.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 3 of 6 - Details

Name: **CVE-2021-4104**

Description: **JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.**

Resolution: **Upgrade package to version greater than 1.2.17**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-4104**

Dependency Root:

Issue 4 of 6

Issue ID:	d43f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	9b3f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/log4j-1.2.16.jar
Line	0
Source File	java_2/lib/log4j-1.2.16.jar
CVSS	8.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 4 of 6 - Details

Name: **CVE-2022-23302**

Description: **JMSSink in all versions of Log4j 1.x is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration or if the configuration references an LDAP service the attacker has access to. The attacker can provide a TopicConnectionFactoryBindingName configuration causing JMSSink to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-4104. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.**

Resolution: **Upgrade package to version greater than 1.2.17**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-23302**

Dependency Root:

Issue 5 of 6

Issue ID:	dc3f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	9b3f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/log4j-1.2.16.jar
Line	0
Source File	java_2/lib/log4j-1.2.16.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 5 of 6 - Details

Name: **CVE-2023-26464**

Description: **** UNSUPPORTED WHEN ASSIGNED ****

**When using the Chainsaw or SocketAppender components with Log4j 1.x on JRE less than 1.7, an attacker that manages to cause a logging entry involving a specially-crafted (ie, deeply nested)
hashmap or hashtable (depending on which logging component is in use) to be processed could exhaust the available memory in the virtual machine and achieve Denial of Service when the object is deserialized.**

This issue affects Apache Log4j before 2. Affected users are recommended to update to Log4j 2.x.

NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

Resolution: **Upgrade package to version greater than or equal to 2.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2023-26464**

Dependency Root:

Issue 6 of 6

Issue ID:	de3f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	9b3f443e-f36b-1410-81f1-00524afcd01d
Location	java_2/lib/log4j-1.2.16.jar
Line	0
Source File	java_2/lib/log4j-1.2.16.jar
CVSS	8.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 6 of 6 - Details

Name: **CVE-2022-23307**

Description: **CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.**

Resolution: **Upgrade package to version greater than or equal to 2.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-23307**

Dependency Root:

C	Common Open Source: Open Source Component: log4j:log4j
Fix Group ID:	a73f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	log4j:log4j
Library Version:	1.2.16
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 6

Issue ID:	c83f443e-f36b-1410-81f1-00524afcd01d
Severity:	Critical
Status	Open
Fix Group ID:	a73f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/log4j-1.2.16.jar
Line	0
Source File	java_1/lib/log4j-1.2.16.jar
CVSS	9.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 6 - Details

Name: **CVE-2019-17571**

Description: **Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.**

Resolution: **Upgrade package to version greater than 1.2.27**

URL: **https://www.cve.org/CVERecord?id=CVE-2019-17571**

Dependency Root:

Issue 2 of 6

Issue ID:	f23f443e-f36b-1410-81f1-00524afcd01d
Severity:	Critical
Status	Open
Fix Group ID:	a73f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/log4j-1.2.16.jar
Line	0
Source File	java_1/lib/log4j-1.2.16.jar
CVSS	9.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 6 - Details

Name: **CVE-2022-23305**

Description: **By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unintended SQL queries to be executed. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default. Beginning in version 2.0-beta8, the JDBCAppender was re-introduced with proper support for parameterized SQL queries and further customization over the columns written to in logs. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.**

Resolution: **Upgrade package to version greater than 1.2.17**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-23305**

Dependency Root:

Issue 3 of 6

Issue ID:	ca3f443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Fix Group ID:	a73f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/log4j-1.2.16.jar
Line	0
Source File	java_1/lib/log4j-1.2.16.jar
CVSS	8.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 3 of 6 - Details

Name: **CVE-2022-23302**

Description: **JMSSink in all versions of Log4j 1.x is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration or if the configuration references an LDAP service the attacker has access to. The attacker can provide a TopicConnectionFactoryBindingName configuration causing JMSSink to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-4104. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.**

Resolution: **Upgrade package to version greater than 1.2.17**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-23302**

Dependency Root:

Issue 4 of 6

Issue ID:	bc3f443e-f36b-1410-81f1-00524afcd01d
Severity:	**High**
Status	Open
Fix Group ID:	a73f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/log4j-1.2.16.jar
Line	0
Source File	java_1/lib/log4j-1.2.16.jar
CVSS	8.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 4 of 6 - Details

Name: **CVE-2022-23307**

Description: **CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.**

Resolution: **Upgrade package to version greater than or equal to 2.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-23307**

Dependency Root:

Issue 5 of 6

Issue ID:	ea3f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	a73f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/log4j-1.2.16.jar
Line	0
Source File	java_1/lib/log4j-1.2.16.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 5 of 6 - Details

Name: **CVE-2023-26464**

Description: **** UNSUPPORTED WHEN ASSIGNED ****

**When using the Chainsaw or SocketAppender components with Log4j 1.x on JRE less than 1.7, an attacker that manages to cause a logging entry involving a specially-crafted (ie, deeply nested)
hashmap or hashtable (depending on which logging component is in use) to be processed could exhaust the available memory in the virtual machine and achieve Denial of Service when the object is deserialized.**

This issue affects Apache Log4j before 2. Affected users are recommended to update to Log4j 2.x.

NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

Resolution: **Upgrade package to version greater than or equal to 2.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2023-26464**

Dependency Root:

Issue 6 of 6

Issue ID:	ec3f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	a73f443e-f36b-1410-81f1-00524afcd01d
Location	java_1/lib/log4j-1.2.16.jar
Line	0
Source File	java_1/lib/log4j-1.2.16.jar
CVSS	7.5
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 6 of 6 - Details

Name: **CVE-2021-4104**

Description: **JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.**

Resolution: **Upgrade package to version greater than 1.2.17**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-4104**

Dependency Root:

H	Common Open Source: Open Source Component: setuptools
Fix Group ID:	a13f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	setuptools
Library Version:	65.5.0
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 2

Issue ID:	da3f443e-f36b-1410-81f1-00524afcd01d
Severity:	High
Status	Open
Fix Group ID:	a13f443e-f36b-1410-81f1-00524afcd01d
Location	python-SCA-CVE/SCA-CVE/app/requirements.txt
Line	0
Source File	python-SCA-CVE/SCA-CVE/app/requirements.txt
CVSS	8.8
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 2 - Details

Name: **CVE-2024-6345**

Description: **setuptools vulnerable to Command Injection via package URL**

Resolution: **Upgrade package to version greater than or equal to 70.0.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2024-6345**

Dependency Root:

Issue 2 of 2

Issue ID:	fc3f443e-f36b-1410-81f1-00524afcd01d
Severity:	Medium
Status	Open
Fix Group ID:	a13f443e-f36b-1410-81f1-00524afcd01d
Location	python-SCA-CVE/SCA-CVE/app/requirements.txt
Line	0
Source File	python-SCA-CVE/SCA-CVE/app/requirements.txt
CVSS	5.9
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 2 of 2 - Details

Name: **CVE-2022-40897**

Description: **Python Packaging Authority (PyPA) setuptools before 65.5.1 allows remote attackers to cause a denial of service via HTML in a crafted package or custom PackageIndex page. There is a Regular Expression Denial of Service (ReDoS) in package_index.py.**

Resolution: **Upgrade package to version greater than or equal to 65.5.1**

URL: **https://www.cve.org/CVERecord?id=CVE-2022-40897**

Dependency Root:

L Common Open Source: Open Source Component: pip

Fix Group ID:	9e3f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	pip
Library Version:	22.3.1
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 1

Issue ID:	be3f443e-f36b-1410-81f1-00524afcd01d
Severity:	Low
Status	Open
Fix Group ID:	9e3f443e-f36b-1410-81f1-00524afcd01d
Location	python-SCA-CVE/SCA-CVE/app/requirements.txt
Line	0
Source File	python-SCA-CVE/SCA-CVE/app/requirements.txt
CVSS	3.3
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 1 - Details

Name: **CVE-2023-5752**

Description: **When installing a package from a Mercurial VCS URL (ie "pip install hg+...") with pip prior to v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options to the "hg clone" call (ie "--config"). Controlling the Mercurial configuration can modify how and which repository is installed. This vulnerability does not affect users who aren't installing from Mercurial.**

Resolution: **Upgrade package to version greater than or equal to 23.3**

URL: **https://www.cve.org/CVERecord?id=CVE-2023-5752**

Dependency Root:

C Common Open Source: Open Source Component: httpx

Fix Group ID:	ad3f443e-f36b-1410-81f1-00524afcd01d
Status:	Open
Date:	2025-07-16 08:17:08Z
Library name:	httpx
Library Version:	0.28.1
How to Fix:	Open Source Component See also issue-details 'Resolution' section below.

Issue 1 of 1

Issue ID:	e43f443e-f36b-1410-81f1-00524afcd01d
Severity:	**Critical**
Status	Open
Fix Group ID:	ad3f443e-f36b-1410-81f1-00524afcd01d
Location	python-SCA-CVE/SCA-CVE/app/requirements.txt
Line	0
Source File	python-SCA-CVE/SCA-CVE/app/requirements.txt
CVSS	9.1
Date Created	Wednesday, July 16, 2025
Last Updated	Wednesday, July 16, 2025
CWE:	829

Issue 1 of 1 - Details

Name: **CVE-2021-41945**

Description: **Encode OSS httpx < 0.23.0 is affected by improper input validation in `httpx.URL`, `httpx.Client` and some functions using `httpx.URL.copy_with`.**

Resolution: **Upgrade package to version greater than 1.0.0**

URL: **https://www.cve.org/CVERecord?id=CVE-2021-41945**

Dependency Root:

How to Fix

C 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