SBOM360 Generated Security Assessment Report

PROJECT: ALPINE-VULN2.31.2

REPORT GENERATED DATE: Apr 07, 2025

This assessment report provides details on Software Supply Chain risks after analyzing library/alpine for alpine, Vuln2.31.2. This report should be used to analyze the risks brought in by Open-Source usage, prioritize resources to effectively address the risks in the supply chain.

Security Assessment Report

PROJECT: ALPINE

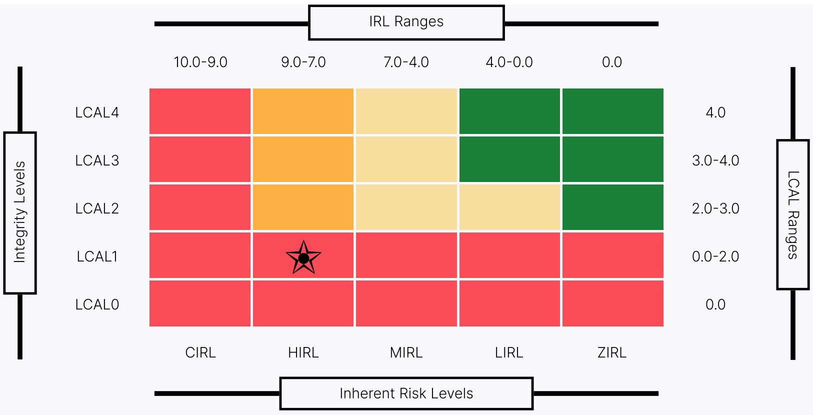
VERSION: VULN2.31.2

INPUT DETAILS: library/alpine

INPUT TYPE: DOCKERHUB

CREATOR: deepak_bharadwaj@lineaje.com

CREATED: Apr 02, 2025



Number of Components

16

Mean Inherent Risk Level of Components (IRL)

(🟧 High 8.1)

Mean Component Attestation Level

(🟥 Unknown 0.88)

Range of IRL

Inherent Risk Level (IRL)	Description	Number of Components
Zero Inherent Risk Level (0)	Average risk score of all components across all four contributors is zero.	**0**
Low Inherent Risk Level (0.1 to 3.9)	Average risk score of all components across all four contributors is between 0.1 and 3.9.	**0**
Medium Inherent Risk Level (4 to 6.9)	Average risk score of all components across all four contributors is between 4 and 6.9.	**14**
High Inherent Risk Level (7 to 8.9)	Average risk score of all components across all four contributors is between 7 and 8.9.	**2**
Critical Inherent Risk Level (9 to 10)	Average risk score of all components across all four contributors is between 9.0 and 10	**0**

Range of LCAL

Lineaje Component Attestation Level (LCAL)	Description	Number of Components
LCAL 0 Unknown Component	The component package cannot be resolved to any known package	**9**
LCAL 1 Known Component	The component name, PURL are traceable and attestable. The package may be available at the PURL but the fingerprint doesn't match.	**0**
LCAL 2 Attested Component	The component name, PURL are traceable and attestable. The package may be available at the PURL and the fingerprint matches.	**7**
LCAL 3 Attested Build & Source	The component package is 'Attested', its source exists and the package is attested to be built from the source	**0**
LCAL 4 Fully Attested	Package and source are attested to be untampered and malware free. There is no malicious code or tamper that was introduced in the original source or between the source and the built output.	**0**

Security Assessment Report

PROJECT: ALPINE	**VERSION:** VULN2.31.2
INPUT DETAILS: library/alpine	**INPUT TYPE:** DOCKERHUB
CREATOR: deepak_bharadwaj@lineaje.com	**CREATED:** Apr 02, 2025

Assessment Summary

Component Origin

7 Open Source	0 Private
9 Third Party	0 Unknown

Dependency Tree

1 Direct	0 Unknown
15 Transitive	2 Depth

Component Age

16 🟥 > 36 months	0 🟨 18-24 months
0 🟧 24-36 months	0 🟩 5-18 months

Vulnerability Severity

0 🟥 Critical (CVSS 9.0 - 10.0)	4 🟨 Medium (CVSS 3.0 - 6.9)
2 🟧 High (CVSS 7.0 - 8.9)	0 🟩 Low (Upto 2.9)

Security Posture

0 🟥 Critical	0 🟨 Medium
0 🟧 High	0 🟩 Low

Code Quality

0 🟥 Critical	0 🟨 Medium
0 🟧 High	0 🟩 Low

Language Distribution

Vulnerability Origin

0 Open Source	0 Private
4 Third Party	0 Unknown

Geo Provenance

Component Maintainability

16
Un-maintained Components

0
Well-maintained Components

Suppliers

15
Total Suppliers

License

6
Total Project License

Security Assessment Report

PROJECT: ALPINE

VERSION: VULN2.31.2

INPUT DETAILS: library/alpine

INPUT TYPE: DOCKERHUB

CREATOR: deepak_bharadwaj@lineaje.com

CREATED: Apr 02, 2025

Component Origin and Maintenance Status

Only Direct and first level transitive dependencies can be safely patched by developers. Additionally, upgrading direct dependencies, as well as patching, updating, or upgrading deep transitive dependencies requires incremental compatibility testing. Unplanned upgrades add an overhead of 40% in software maintenance.

Unmaintained Open-Source components are components that are no longer maintained, where the most recent version of the component available is greater than 2 years old.

Well-Maintained Open-Source components are components that have been updated in the past 6 months, the most recent version of the component is less than 6 months old.

Origin	Total Components	Direct Dependencies	Transitive Dependencies	Unmaintained Components	Well-maintained Components
Open Source	7	1	6	7	0
Third Party	9	0	9	9	0
Private	0	0	0	0	0
Unknown	0	0	0	0	0

Component Origin and Maintenance Status

Origin	Description	Direct Dependencies
Open Source	Older than 36 months Released 24-36 months ago Released 18-24 months ago Released 5-18 months ago	**7** **0** **0** **0**
Third Party	Older than 36 months Released 24-36 months ago Released 18-24 months ago Released 5-18 months ago	**9** **0** **0** **0**
Private	Older than 36 months Released 24-36 months ago Released 18-24 months ago Released 5-18 months ago	**0** **0** **0** **0**
Unknown	Older than 36 months Released 24-36 months ago Released 18-24 months ago Released 5-18 months ago	**0** **0** **0** **0**

Security Assessment Report

PROJECT: ALPINE

VERSION: VULN2.31.2

INPUT DETAILS: library/alpine

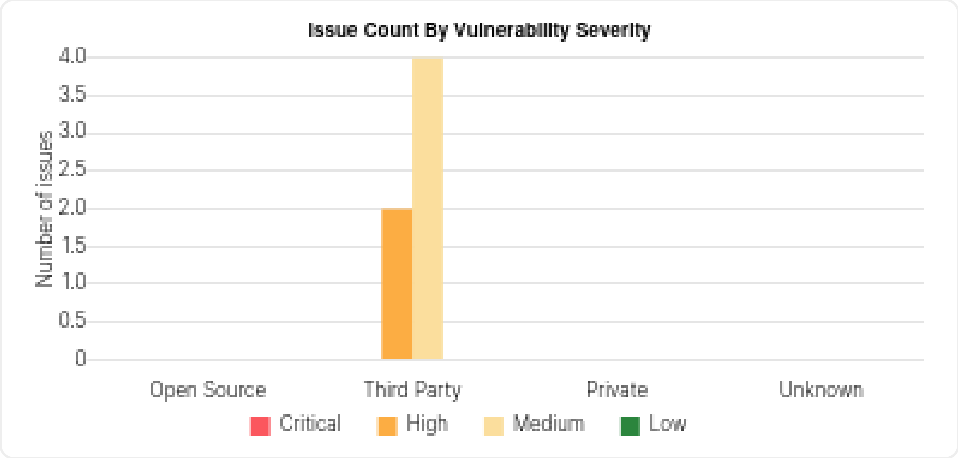
INPUT TYPE: DOCKERHUB

CREATOR: deepak_bharadwaj@lineaje.com

CREATED: Apr 02, 2025

Vulnerability Analysis

Vulnerabilities in Open-Source components refer to weaknesses or flaws within the software that can be exploited by attackers to compromise the security or functionality of a system.



Vulnerability Fixed State	Component Maintainability	Count
Fixed	Unmaintained Well-maintained	4 0
Not fixed	Unmaintained Well-maintained	0 0

Vulnerability Severity	Component Age Range	Count
Critical	Older than 3 years Released between 2 to 3 years Released between 18 - 24 months Released between 5 - 18 months	0 0 0 0
High	Older than 3 years Released between 2 to 3 years Released between 18 - 24 months Released between 5 - 18 months	2 0 0 0
Medium	Older than 3 years Released between 2 to 3 years Released between 18 - 24 months Released between 5 - 18 months	4 0 0 0
Low	Older than 3 years Released between 2 to 3 years Released between 18 - 24 months Released between 5 - 18 months	0 0 0 0

Vulnerability Fix State	Exploitability	Component Origin	Count
Fixed	Exploited	Open-Source Third-Party Private Unknown	0 0 0 0
Fixed	Not exploited	Open-Source Third-Party Private Unknown	0 6 0 0
Not Fixed	Exploited	Open-Source Third-Party Private Unknown	0 0 0 0
Not Fixed	Not exploited	Open-Source Third-Party Private Unknown	0 0 0 0

Security Assessment Report

PROJECT: ALPINE

VERSION: VULN2.31.2

INPUT DETAILS: library/alpine

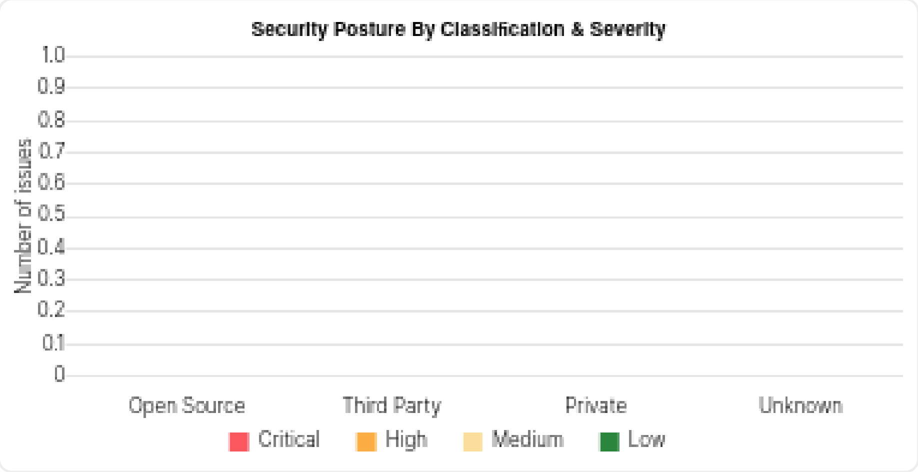
INPUT TYPE: DOCKERHUB

CREATOR: deepak_bharadwaj@lineaje.com

CREATED: Apr 02, 2025

Security Posture Analysis

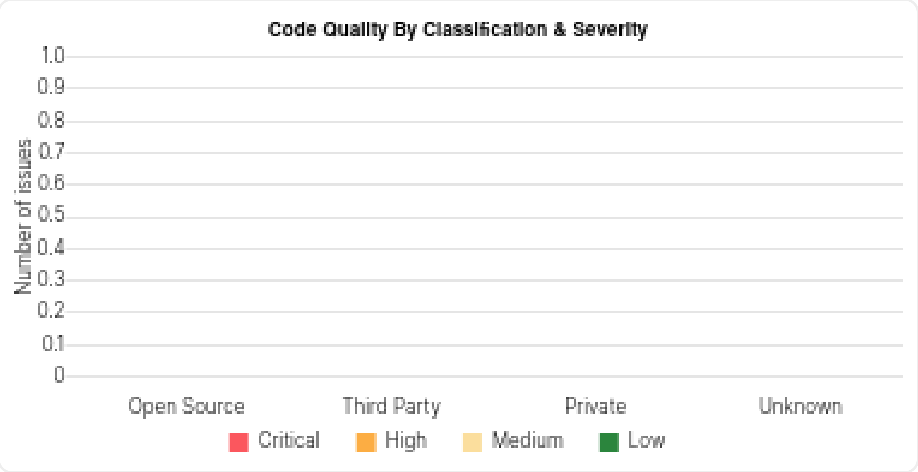
Security posture is calculated by running a set of checks on the source code of each component. This includes direct and transitive dependencies. Refer this link for the list of checks performed.



Issue Severity	Component Origin	Count
Critical	Open-Source Third-Party Private Unknown	0 0 0 0
High	Open-Source Third-Party Private Unknown	0 0 0 0
Medium	Open-Source Third-Party Private Unknown	0 0 0 0
Low	Open-Source Third-Party Private Unknown	0 0 0 0

Code Quality Analysis

Code quality is calculated by running a set of checks on the source code of each component. This includes direct and transitive dependencies. Refer this link for the list of checks performed.



Issue Severity	Component Origin	Count
Critical	Open-Source Third-Party Private Unknown	0 0 0 0
High	Open-Source Third-Party Private Unknown	0 0 0 0
Medium	Open-Source Third-Party Private Unknown	0 0 0 0
Low	Open-Source Third-Party Private Unknown	0 0 0 0

Geographic Provenance

The analysis of geographical and authorial origins of the software components to track their sources and identify potential risks. The table below summarizes the code commits by authors geographic provenance.

Top 6 Code Commits By Country	Percentage

Security Assessment Report

PROJECT: ALPINE

VERSION: VULN2.31.2

INPUT DETAILS: library/alpine

INPUT TYPE: DOCKERHUB

CREATOR: deepak_bharadwaj@lineaje.com

CREATED: Apr 02, 2025

Riskiest Component in the Project

The level of risk is determined by evaluating the presence of vulnerabilities in components, the degree of code maintainability, the overall security posture, and the quality of the codebase.

Top 10 Riskiest Components	Risk Score	Risk Severity	Vulnerabilities	Component Age Range
alpine:musl:1.2.5-r8	8.1	High	1	> 36 Months
alpine:musl-utils:1.2.5-r8	8.1	High	1	> 36 Months
alpine:busybox:1.37.0-r9	6.9	Medium	0	> 36 Months
alpine:libcrypto3:3.3.2-r4	6.9	Medium	2	> 36 Months
alpine:ssl_client:1.37.0-r9	6.9	Medium	0	> 36 Months
alpine:alpine-release:3.21.2-r0	6.9	Medium	0	> 36 Months
oci:alpine:sha256:56fa17d2a7e7f168a043a2712e63aed1f8543aeafdcee47c58dcffe38ed51099	6.9	Medium	0	> 36 Months
alpine:alpine-keys:2.5-r0	6.9	Medium	0	> 36 Months
alpine:alpine-baselayout:3.6.8-r1	6.9	Medium	0	> 36 Months
alpine:busybox-binsh:1.37.0-r9	6.9	Medium	0	> 36 Months

Top 10 Known Unknown Components in the Project

Known Unknown Component: A component is considered a known unknown if its name and package URL (PURL) are traceable and attestable. While the package may be available at the PURL location, the component is classified as known even if the package fingerprint does not match.

Top 10 Known Unknown Components	PURL	Risk Attestation Level	Package Manager	Classification	Supplier
alpine:busybox:1.37.0-r9	pkg:apk/alpine/busybox@1.37.0-r9?arch=x86_64&distro=alpine-3.21.2	0	apk	TP	Alpine
alpine:libcrypto3:3.3.2-r4	pkg:apk/alpine/libcrypto3@3.3.2-r4?arch=x86_64&distro=alpine-3.21.2&upstream=openssl	0	apk	TP	Alpine
alpine:ssl_client:1.37.0-r9	pkg:apk/alpine/ssl_client@1.37.0-r9?arch=x86_64&distro=alpine-3.21.2&upstream=busybox	0	apk	TP	Alpine
alpine:alpine-release:3.21.2-r0	pkg:apk/alpine/alpine-release@3.21.2-r0?arch=x86_64&distro=alpine-3.21.2&upstream=alpine-base	0	apk	TP	Alpine
alpine:busybox-binsh:1.37.0-r9	pkg:apk/alpine/busybox-binsh@1.37.0-r9?arch=x86_64&distro=alpine-3.21.2&upstream=busybox	0	apk	TP	Alpine
alpine:libssl3:3.3.2-r4	pkg:apk/alpine/libssl3@3.3.2-r4?arch=x86_64&distro=alpine-3.21.2&upstream=openssl	0	apk	TP	Alpine
alpine:musl:1.2.5-r8	pkg:apk/alpine/musl@1.2.5-r8?arch=x86_64&distro=alpine-3.21.2	0	apk	TP	Alpine
alpine:musl-utils:1.2.5-r8	pkg:apk/alpine/musl-utils@1.2.5-r8?arch=x86_64&distro=alpine-3.21.2&upstream=musl	0	apk	TP	Alpine
alpine:apk-tools:2.14.6-r2	pkg:apk/alpine/apk-tools@2.14.6-r2?arch=x86_64&distro=alpine-3.21.2	0	apk	TP	Alpine

Security Assessment Report

PROJECT: ALPINE

VERSION: VULN2.31.2

INPUT DETAILS: library/alpine

INPUT TYPE: DOCKERHUB

CREATOR: deepak_bharadwaj@lineaje.com

CREATED: Apr 02, 2025

List of Components with NO Fix

#	Package ID	Current Version					
		Version	Total Vulnerabilities	Vulnerabilities Distribution			
				Critical	High	Medium	Low
No Data Available							

Annexure A

Vulnerabilities in your Project

The below table lists down all the vulnerable components in your project. In addition it also provides more information like currently affected version and the related vulnerability details like CVE number, CVE score and severity. For each of these listed vulnerable components table also provides you details on any available fixes. CVE fix versions are just indications of versions in which CVEs are addressed. Care must be taken to pick the right version to ensure compatibility of the new version across the dependency tree.

#	Package ID	Version	Vulnerability Name	Severity	CVSS Score	Vulnerability Vector	Fixed State	Fixed in Version
1	alpine:libcrypto3:3.3.2-r4	3.3.2-r4	CVE-2024-12797	Medium	6.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L /A:L	fixed	3.3.3-r0
2	alpine:libcrypto3:3.3.2-r4	3.3.2-r4	CVE-2024-13176	Medium	4.1	CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:L/I:L /A:L	fixed	3.3.2-r5
3	alpine:musl:1.2.5-r8	1.2.5-r8	CVE-2025-26519	High	8.1	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H /A:L	fixed	1.2.5-r9
4	alpine:musl-utils:1.2.5-r8	1.2.5-r8	CVE-2025-26519	High	8.1	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H /A:L	fixed	1.2.5-r9
5	alpine:libssl3:3.3.2-r4	3.3.2-r4	CVE-2024-12797	Medium	6.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L /A:L	fixed	3.3.3-r0
6	alpine:libssl3:3.3.2-r4	3.3.2-r4	CVE-2024-13176	Medium	4.1	CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:L/I:L /A:L	fixed	3.3.2-r5

Annexure B

Components in your project

#	Component name	Component Version	Vulnerability Count
1	pkg:apk/alpine/libcrypto3	3.3.2-r4	2
2	pkg:apk/alpine/ca-certificates-bundle	20241121-r1	0
3	pkg:oci/alpine	56fa17d2a7e7f168a043a2712e63aed1f8543aeafdcee47c58dcffe38ed51099	0
4	pkg:apk/alpine/ssl_client	1.37.0-r9	0
5	pkg:apk/alpine/busybox-binsh	1.37.0-r9	0
6	pkg:apk/alpine/alpine-keys	2.5-r0	0
7	pkg:apk/alpine/alpine-baselayout-data	3.6.8-r1	0
8	pkg:apk/alpine/apk-tools	2.14.6-r2	0
9	pkg:apk/alpine/alpine-release	3.21.2-r0	0
10	pkg:apk/alpine/busybox	1.37.0-r9	0
11	pkg:apk/alpine/zlib	1.3.1-r2	0
12	pkg:apk/alpine/scanelf	1.3.8-r1	0
13	pkg:apk/alpine/musl	1.2.5-r8	1
14	pkg:apk/alpine/musl-utils	1.2.5-r8	1
15	pkg:apk/alpine/alpine-baselayout	3.6.8-r1	0
16	pkg:apk/alpine/libssl3	3.3.2-r4	2