

{metæffekt}

Keycloak

Vulnerability Report

Asset:	Keycloak	Classification:	Public
Version:	25.0.4	Supplier:	metæffekt GmbH
Asset Identifier:	quay.io/keycloak/keycloak	Contact:	contact@metæffekt.com
Asset Type:	Container	Date:	12.09.2024
Environment:	undefined	Status:	Preview

metæffekt GmbH
<https://metæffekt.com>

Imprint

Example

Version: 1.0

Keycloak

Version: 25.0.4
Date: 12.09.2024

Vulnerability Report

Version: 0.1
Status: Preview
Classification: Public
Date: 12.09.2024

Copyright 2024, metæffekt GmbH

metæffekt GmbH

<https://metæffekt.com>

Notice

Names and Trademarks

All company names, organization names, and product names mentioned in this documentation are used for identification purposes only. A trademark is explicitly identified as registered or unregistered trademark only if required by appropriate guidelines or license terms.

External Vulnerability Materials

Materials - including data, content, and references - covering vulnerability information from external sources are presented in this documentation 'AS IS'. metæffekt GmbH does not claim any copyright on the included external materials nor is metæffekt GmbH liable for the correctness and completeness of the presented external materials. Materials from external sources are included herein for informational purposes only. metæffekt GmbH is not responsible for the availability and content provided by external links.

Third-Party Component Vulnerabilities

The vulnerabilities enlisted within this document are primarily vulnerabilities of third-party software or hardware components that are included within or integrated with assets of metæffekt GmbH. The fact that such a component has a known vulnerability must not necessarily mean that this vulnerability immediately affects the metæffekt GmbH assets. Vulnerabilities need to be categorized and assessed within the context of the asset using the affected components.

Vulnerability Categories

Vulnerabilities of included or integrated third-party components are categorized in three categories:

- **Potential Vulnerabilities** affect functions or interfaces used by the metæffekt GmbH assets and require an individual assessment. Whether a vulnerability imposes a risk on the availability, integrity and/or confidentiality of data being processed, or functions being executed by the asset is subject to an individual assessment.
- **Not Applicable Vulnerabilities** are vulnerabilities that are associated with an included or integrated third-party component, but only affect functions or interfaces that are not in use or deactivated. For not applicable vulnerabilities a rationale is provided explaining why the vulnerability does not affect a given asset.
- **Insignificant Vulnerabilities** are either vulnerabilities below a given vulnerability score threshold or have been degraded during an assessment in a given context. Insignificant vulnerabilities are nevertheless listed to provide a comprehensive view. A rationale is provided in case a vulnerability was degraded to an insignificant vulnerability during the vulnerability assessment.

Insignificant Vulnerabilities Threshold

In general, only vulnerabilities with Score_{\max} higher or equal a threshold of \$threshold are considered relevant in the given context. Vulnerabilities with Score_{\max} lower than \$threshold are categorized as insignificant vulnerabilities by default.

Vulnerability Assessment

Identified vulnerabilities are assessed in four major steps:

1. Correlation Verification - The identified components are automatically correlated with vulnerable products. The correlation may be false, incomplete, or imprecise. In the correlation verification step the automated mapping is reviewed and improved. Based on a precise vulnerable product correlation vulnerabilities can be queried more accurately.
2. Applicability Check - Queried vulnerabilities are analyzed for applicability. Vulnerabilities that are not applicable are documented by providing an appropriate rationale. Furthermore, vulnerabilities can be degraded or escalated within the given categories.
3. Avoidance Check - For applicable vulnerabilities alternatives or upgrade options are validated. When a defect causing the vulnerability is fixed by a newer version of the component, the update or upgrade options are evaluated within the current development and release timelines.

4. Risk Assessment – Applicable vulnerabilities that cannot be addressed by updating, upgrading or replacements are assessed to determine the imposed security risk. The vulnerability induced risk is described and counter measures for the asset in operation are evaluated and documented.

Vulnerability Severity Metrics

Generally, vulnerability severity is measured using the [Common Vulnerability Scoring System \(CVSS\)](#) scoring system. Currently two versions of the CVSS scoring system are commonly applied. This document uses both the CVSS version 2.0 and the CVSS version 3.x.

For comparison of vulnerabilities the overall CVSS scores Score_{\max} - the maximum of CVSS overall score Score_{v2} and Score_{v3} - is used.

The report uses the default CVSS severity scheme as defined in the CVSS 3.1 specification both to CVSS 2.0 and CVSS 3.x scores:

Severity Rating	CVSS Score Range	Remarks
None	0.0	In the CVSS 2.0 specification 0.0 is included in severity rating Low.
Low	0.1 - 3.9	In the CVSS 2.0 specification 0.0 is included in severity rating Low.
Medium	4.0 - 6.9	
High	7.0 - 8.9	In the CVSS 2.0 specification the severity rating Critical does not exist. CVSS scores from 7.0 to 10.0 are all rated as High.
Critical	9.0 - 10.0	In the CVSS 2.0 specification the severity rating Critical does not exist. CVSS scores from 7.0 to 10.0 are all rated as High.

Table 1: CVSS Severity Scheme

External Vulnerability Sources

The [National Vulnerability Database \(NVD\)](#) is the primary data source for vulnerability information utilized. A vulnerable product is represented within NVD as [Common Product Enumeration \(CPE\)](#); an individual vulnerability as [Common Vulnerability Exposure \(CVE\)](#).

Advisory information is included from additional sources. These vary dependent on the product domain and target audience.

Copyright

This documentation is protected by copyright 2024, metæffekt GmbH.

Contents

Imprint.....	2
Notice.....	3
1 Vulnerability Overview.....	7
2 Vulnerability Statistics.....	8
3 Vulnerability List.....	10
Applicable.....	10
In Review.....	10
Not Applicable.....	12
Insignificant.....	12
Void.....	13
4 Vulnerability Details.....	14
CVE-2023-7104.....	14
CVE-2023-6841.....	16
CVE-2023-5156.....	17
CVE-2023-4911.....	19
CVE-2023-4813.....	21
CVE-2023-45853.....	23
CVE-2023-4527.....	25
CVE-2023-4039.....	27
CVE-2023-29491.....	29
CVE-2023-2603.....	31
CVE-2023-0687.....	32
CVE-2022-41409.....	34
CVE-2022-37832.....	36
CVE-2022-37434.....	38
CVE-2022-35737.....	40
CVE-2022-29458.....	41
CVE-2022-23219.....	43
CVE-2022-23218.....	45
CVE-2021-46848.....	47
CVE-2021-43396.....	49
CVE-2021-3998.....	51
CVE-2021-39537.....	52
CVE-2021-38604.....	54
CVE-2020-25638.....	56
CVE-2020-13956.....	58
CVE-2019-14900.....	59
CVE-2018-25032.....	61
CVE-2018-15529.....	63
CVE-2016-7091.....	65
CVE-2016-2781.....	67
CVE-2013-0136.....	68
CVE-2011-0536.....	70
CVE-2010-4756.....	72

List of Tables.....	75
Glossary.....	82

1 Vulnerability Overview

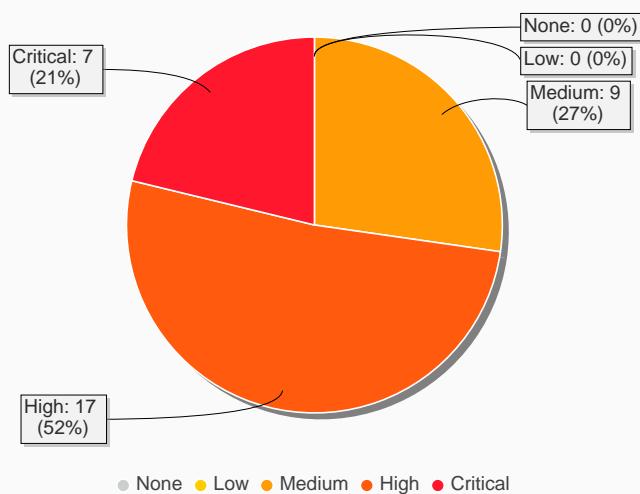
For the third-party components contained in Example vulnerabilities have been queried from public vulnerability databases. The following sections cover the vulnerabilities for the software parts included in Example.

Overview Charts

A set of charts depicts the vulnerabilities correlated with Example. The following illustrations convey insights on the initial vulnerability situation, the assessment status and the severity of the correlated vulnerabilities in the given context.

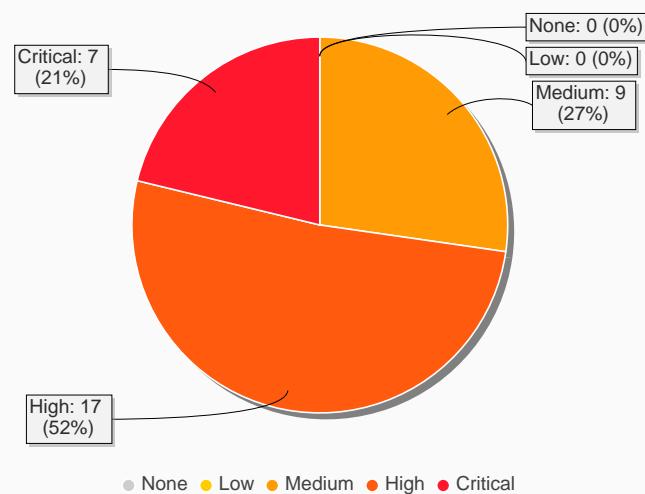
Initial Vulnerability Severity

The chart depicts the vulnerability severity distribution without context information.



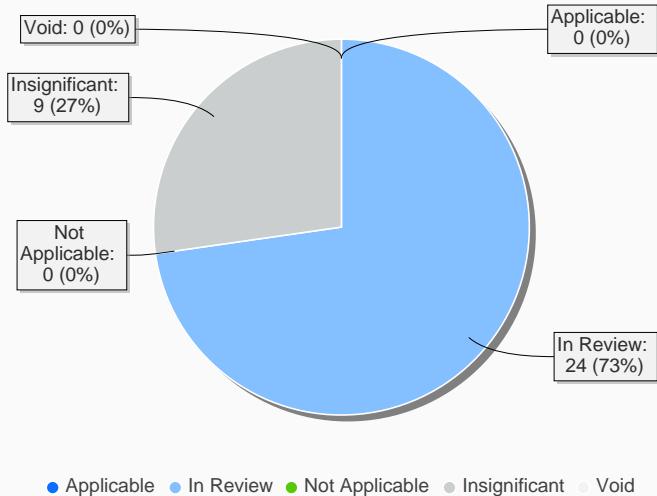
Context Vulnerability Severity

The chart provides the distribution of vulnerability severities after evaluation of the vulnerabilities in the given context.



Vulnerability Assessment Status

The illustration provides information on the current assessment status.



CVSS Severity per Component

The chart visualizes the distribution of vulnerabilities on components included in Example.

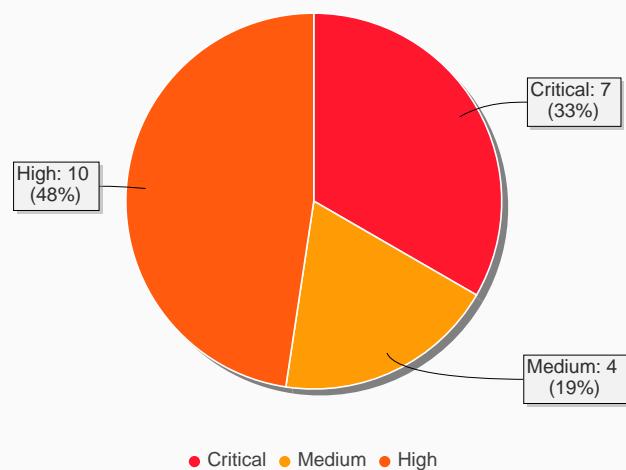


Table 2: Overview Charts

2 Vulnerability Statistics

The following table shows statistics for the identified vulnerabilities. The vulnerabilities are included in the statistics with their original unmodified severity.

Severity	Applicable	In Review	Not Applicable	Insignificant	Void	Total	Assessed
Critical	0	7	0	0	0	7	0,0 %
High	0	17	0	0	0	17	0,0 %
Medium	0	0	0	9	0	9	0,0 %
Low	0	0	0	0	0	0	n/a

Table 3: Vulnerability Statistics

The following table shows statistics for the identified vulnerabilities with advisory information from CERT-EU. The vulnerabilities are included in the statistics with their original unmodified severity.

Severity	Applicable	In Review	Not Applicable	Insignificant	Void	Total	Assessed
Critical	0	0	0	0	0	0	n/a
High	0	1	0	0	0	1	0,0 %
Medium	0	0	0	0	0	0	n/a
Low	0	0	0	0	0	0	n/a

Table 4: Vulnerability Statistics with CERT-EU Advisories

The following table shows statistics for the identified vulnerabilities. The vulnerabilities are included in the statistics with their modified severity if available or their unmodified severity otherwise.

Severity	Applicable	In Review	Not Applicable	Insignificant	Void	Total	Assessed
Critical	0	7	0	0	0	7	0,0 %
High	0	17	0	0	0	17	0,0 %
Medium	0	0	0	9	0	9	0,0 %
Low	0	0	0	0	0	0	n/a

Table 5: Context Vulnerability Statistics

The following table shows statistics for the identified vulnerabilities with advisory information from CERT-EU. The vulnerabilities are included in the statistics with their modified severity if available or their unmodified severity otherwise.

Severity	Applicable	In Review	Not Applicable	Insignificant	Void	Total	Assessed
Critical	0	0	0	0	0	0	n/a
High	0	1	0	0	0	1	0,0 %
Medium	0	0	0	0	0	0	n/a
Low	0	0	0	0	0	0	n/a

Table 6: Context Vulnerability Statistics with CERT-EU Advisories

The following table shows statistics for the identified vulnerabilities from CISA KEV

Exploited in the Wild	Total	Percentage
KNOWN	1	3.0%
UNKNOWN	32	97.0%

Table 7: CISA KEV vulnerabilities statistics

3 Vulnerability List

The following vulnerabilities have been identified and categorized.

Applicable

No vulnerabilities are considered `Applicable` in the given context.

In Review

The following vulnerabilities are considered `In Review` in the given context:

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2023-45853	9.8		Critical		Default	In Review
			GHSA-mq29-j5xf-cjwr			
			cpe:/a:zlib:zlib [, 1.3]			
CVE-2023-0687	9.8		Critical		Default	In Review
			GHSA-5r4p-4pqv-gqhw			
			cpe:/a:gnu:glibc [, 2.38)			
CVE-2022-37832	9.8		Critical		Default	In Review
			GHSA-999r-r2f8-xm55			
			cpe:/a:mutiny:mutiny [, 7.2.0-10855)			
CVE-2022-37434	9.8		Critical		Default	In Review
			GHSA-cfmr-vrgj-vqww			
			cpe:/a:zlib:zlib [, 1.2.12]			
CVE-2022-23219	9.8		Critical		Escalate	In Review
			GHSA-fhxm-4mc9-6jf5			
			cpe:/a:gnu:glibc [, 2.34]			
CVE-2022-23218	9.8		Critical		Escalate	In Review
			GHSA-8g8v-256r-57v7			
			cpe:/a:gnu:glibc [, 2.34]			
CVE-2021-46848	9.1		Critical		Default	In Review
			GHSA-6468-68pw-9chw			
			cpe:/a:gnu:libtasn1 [, 4.19.0)			
CVE-2021-39537	8.8		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2018-15529	8.8		High		Default	In Review
CVE-2013-0136	8.5		High		Escalate	In Review
CVE-2023-4911	7.8		High		Escalate	In Review
CVE-2023-29491	7.8		High		Default	In Review
CVE-2023-2603	7.8		High		Default	In Review
CVE-2023-5156	7.5		High		Due	In Review
CVE-2022-41409	7.5		High		Due	In Review
CVE-2022-35737	7.5		High		Default	In Review
CVE-2021-43396	7.5		High		Escalate	In Review
CVE-2021-3998	7.5		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-38604	7.5		High		Default	In Review
CVE-2018-25032	7.5		High		Default	In Review
CVE-2020-25638	7.4		High		Escalate	In Review
CVE-2023-7104	7.3		High		Default	In Review
CVE-2023-6841	7.1		High		Due	In Review
CVE-2022-29458	7.1		High		Default	In Review

Table 8: In Review Category

Not Applicable

No vulnerabilities are considered `Not Applicable` in the given context.

Insignificant

The following vulnerabilities are considered `Insignificant` in the given context:

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2011-0536	6.9		Medium		Default	Insignificant
CVE-2023-4527	6.5		Medium		Default	Insignificant

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2019-14900	6.5		Medium		Escalate	Insignificant
CVE-2016-2781	6.5		Medium		Default	Insignificant
CVE-2023-4813	5.9		Medium		Default	Insignificant
CVE-2020-13956	5.3		Medium		Default	Insignificant
CVE-2023-4039	4.8		Medium		Default	Insignificant
CVE-2016-7091	4.4		Medium		Elevated	Insignificant
CVE-2010-4756	4.0		Medium		Elevated	Insignificant

Table 9: Insignificant Category

Void

No vulnerabilities are considered `void` in the given context.

4 Vulnerability Details

Details are provided for vulnerabilities which are either potential vulnerabilities or which have third-party advisories.

CVE-2023-7104

Description

A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-7104

Table 10: CVE-2023-7104 References

Affected Components

Component	Artifact Id	Version
sqlite-libs	sqlite-libs-3.34.1	3.34.1

Table 11: CVE-2023-7104 Affected Components

Weakness

CWE-119, CWE-122

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	High
CVSS:2.0	NVD-CNA-VulDB	5.2	AV:A/AC:L/Au:S/C:P/I:P/A:P	Medium

Table 12: CVE-2023-7104 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.3	3.4	3.9
CVSS:2.0	NVD-CNA-VulDB	5.2	6.4	5.1

Table 13: CVE-2023-7104 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-f92h-rw3f-8j92	A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999.	2023-12-29	2023-12-29

Table 14: CVE-2023-7104 Alerts

Assessment

Summary

In Review Default High

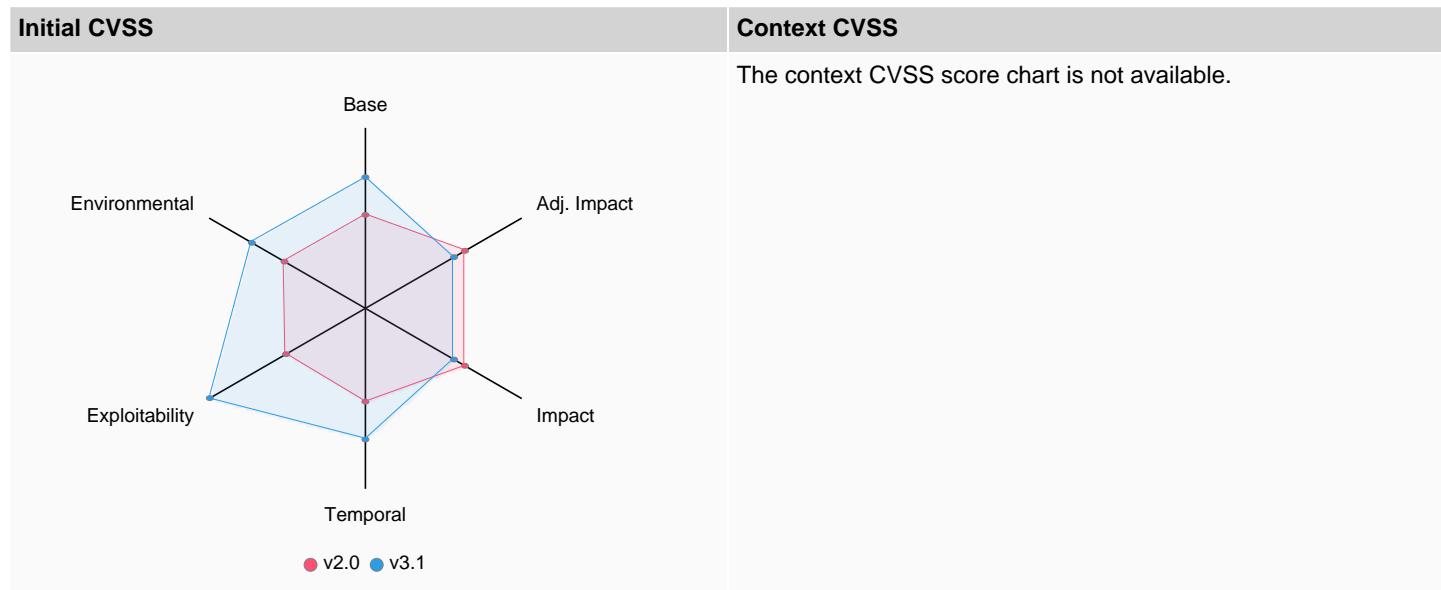


Table 15: CVE-2023-7104 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.

Criteria	Explanation
EOL	sqlite (ver. 3) is still supported by its vendor. Support End Date: no date provided Vendor does not provide extended support for this product.

CVE-2023-6841

Description

A denial of service vulnerability was found in keycloak where the amount of attributes per object is not limited, an attacker by sending repeated HTTP requests could cause a resource exhaustion when the application send back rows with long attribute values.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-6841

Table 16: CVE-2023-6841 References

Affected Components

Component	Artifact Id	Version
	org.keycloak.keycloak-core-25.0.4.jar	25.0.4

Table 17: CVE-2023-6841 Affected Components

Weakness

CWE-231

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:4.0	GitHub, Inc.	7.1	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	High
CVSS:3.1	GitHub, Inc.	6.5	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	Medium

Table 18: CVE-2023-6841 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:4.0	GitHub, Inc.	7.1		
CVSS:3.1	GitHub, Inc.	6.5	3.6	2.8

Table 19: CVE-2023-6841 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-w97f-w3hq-36g2	Keycloak Denial of Service vulnerability	2024-09-10	2024-09-10

Table 20: CVE-2023-6841 Alerts

Assessment

Summary

In Review Due High

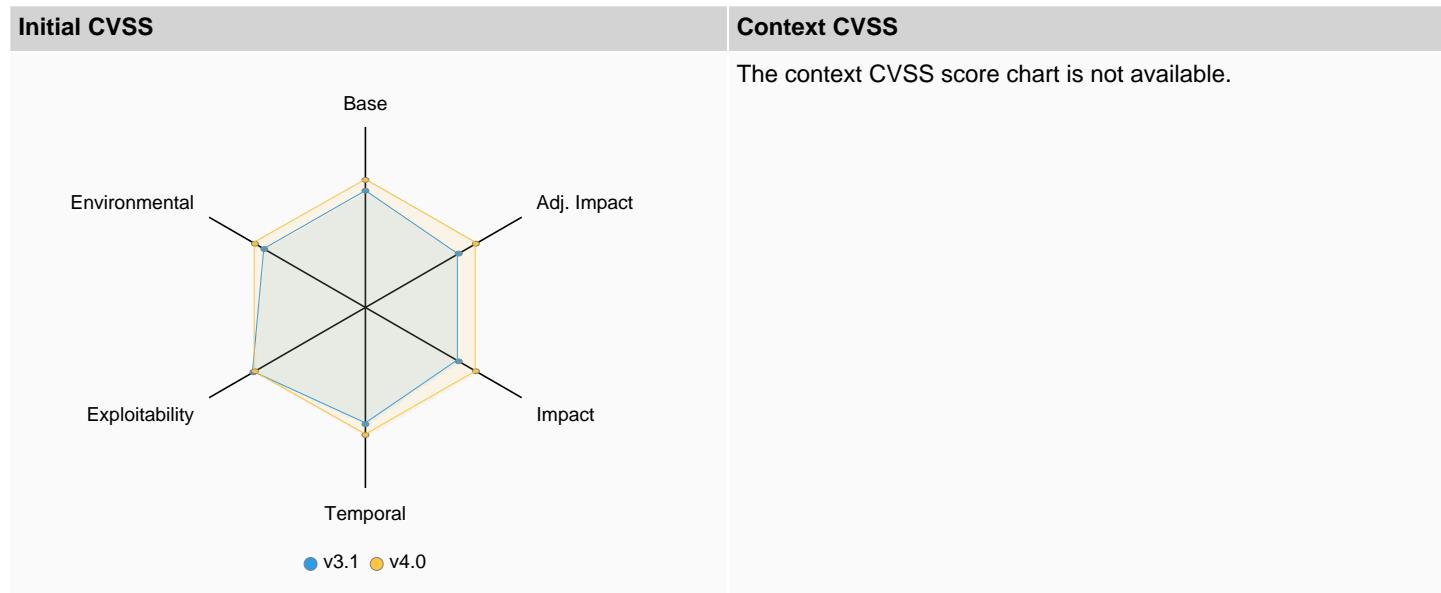


Table 21: CVE-2023-6841 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Due (8.1 from base score 7.1)

Criteria	Explanation
CVSS Overall	CVSS:4.0 GitHub, Inc. provides the vector: <code>CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N</code>
Keywords	resource exemption: An adversary may attempt to exhaust resources of the system compromising performance objectives and availability.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2023-5156

Description

A flaw was found in the GNU C Library. A recent fix for CVE-2023-4806 introduced the potential for a memory leak, which may result in an application crash.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-5156

Table 22: CVE-2023-5156 References

Affected Components

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 23: CVE-2023-5156 Affected Components

Weakness

CWE-401

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	High

Table 24: CVE-2023-5156 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.5	3.6	3.9

Table 25: CVE-2023-5156 Initial Severity Details

Advisories

Alerts

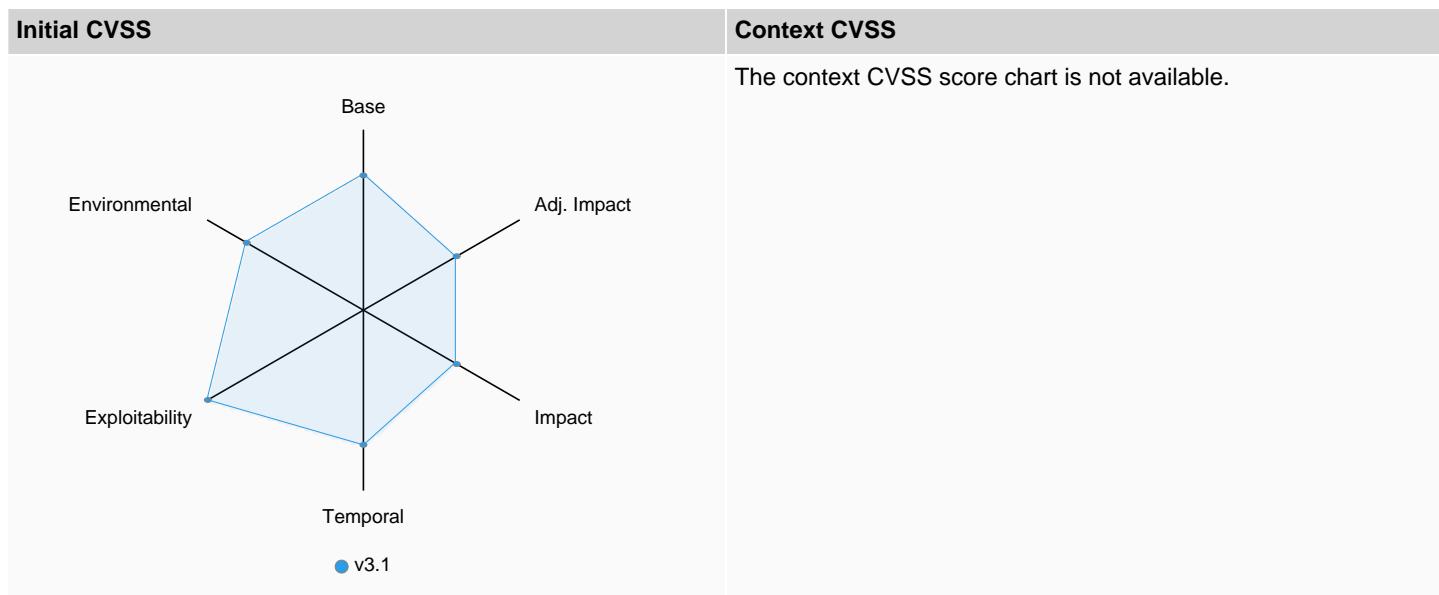
Id	Summary	Create Date	Update Date
GHSA-m7p3-g2hx-xfc3	A flaw was found in the GNU C Library. A recent fix for CVE-2023-4806 introduced the potential for a memory leak, which may result in an application crash.	2023-09-25	2023-09-25

Table 26: CVE-2023-5156 Alerts

Assessment

Summary

In Review Due High

**Table 27: CVE-2023-5156 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Due (8.5 from base score 7.5)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</code>
Keywords	resource exemption: An adversary may attempt to exhaust resources of the system compromising performance objectives and availability.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2023-4911**Description**

A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-4911

Table 28: CVE-2023-4911 References**Affected Components**

Component	Artifact Id	Version
glibc	glibc-2.34	2.34

Component	Artifact Id	Version
glibc-common	glibc-common-2.34	2.34
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 29: CVE-2023-4911 Affected Components**Weakness**

CWE-787, CWE-122

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	High

Table 30: CVE-2023-4911 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.8	5.9	1.8

Table 31: CVE-2023-4911 Initial Severity Details**Advisories****Alerts**

ID	Summary	Create Date	Update Date
CERT-EU-2023-072	GNU C Library Dynamic Loader Buffer Overflow Vulnerability	2023-10-04	2023-10-04
GHSA-m77w-6vjw-wh2f	A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.	2023-10-03	2023-10-03

Table 32: CVE-2023-4911 Alerts**Assessment****Summary**
In Review
Escalate
High

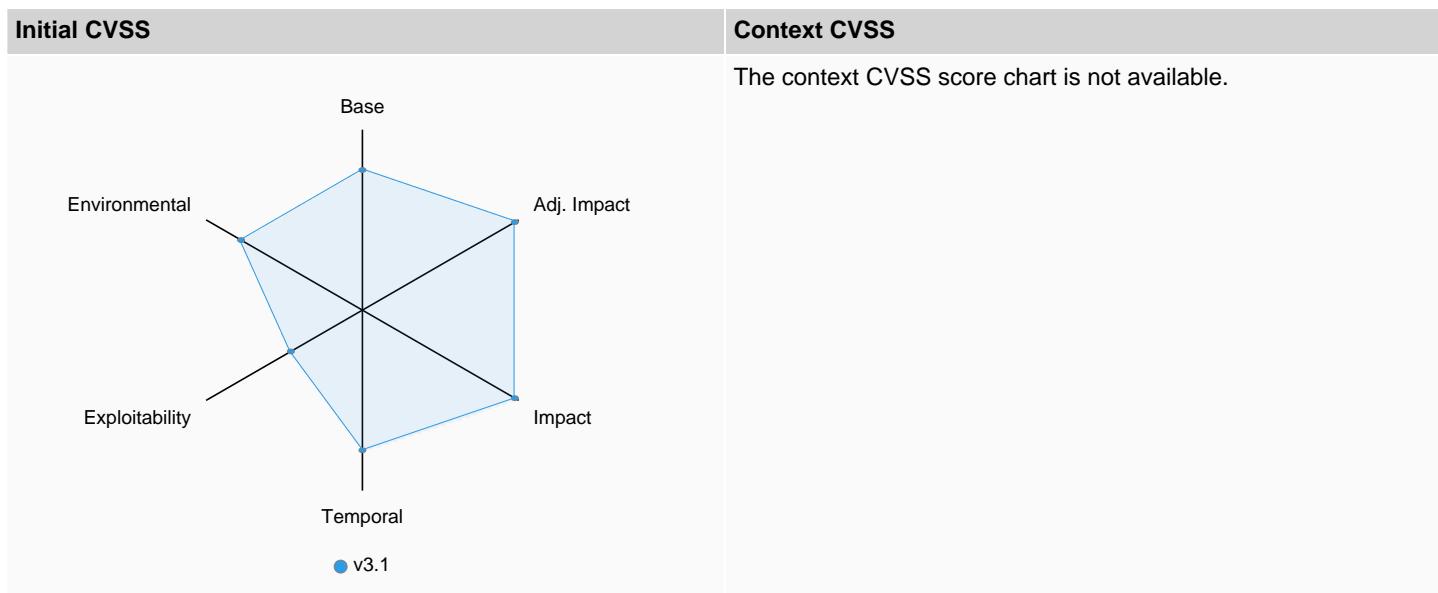


Table 33: CVE-2023-4911 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (9.8 from base score 7.8)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</code>
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability, affecting GNU C Library , has been confirmed to have been exploited in the wild . Summary: GNU C Library Buffer Overflow Vulnerability. Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Notes: This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: https://sourceware.org/git/?p=glibc.git;a=commitdiff;h=1056e5b4c3f2d90ed2b4a55f96add28da2f4c8fa , https://access.redhat.com/security/cve/cve-2023-4911 , https://www.debian.org/security/2023/dsa-5514 ; https://nvd.nist.gov/vuln/detail/CVE-2023-4911 Due Date: 2023-12-12 Publish Date: 2023-11-21
EOL	No EOL information available.

CVE-2023-4813

Description

A flaw was found in glibc. In an uncommon situation, the `gaih_inet` function may use memory that has been freed, resulting in an application crash. This issue is only exploitable when the `getaddrinfo` function is called and the hosts database in `/etc/nsswitch.conf` is configured with `SUCCESS=continue` or `SUCCESS=merge`.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-4813

Table 34: CVE-2023-4813 References**Affected Components**

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 35: CVE-2023-4813 Affected Components**Weakness**

CWE-416

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	Medium

Table 36: CVE-2023-4813 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	5.9	3.6	2.2

Table 37: CVE-2023-4813 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-qx6j-g797-jg9r	A flaw was found in glibc. In an uncommon situation, the <code>gaih_inet</code> function may use memory that has been freed, resulting in an application crash. This issue is only exploitable when the <code>getaddrinfo</code> function is called and the hosts database in <code>/etc/nsswitch.conf</code> is configured with <code>SUCCESS=continue</code> or <code>SUCCESS=merge</code> .	2023-09-13	2023-09-13

Table 38: CVE-2023-4813 Alerts**Assessment****Summary**

Insignificant	Default	Medium
---------------	---------	--------

Initial CVSS	Context CVSS
<p>The diagram shows a diamond-shaped vector space for CVSS 3.1. The vertical axis is labeled 'Base'. The horizontal axis is labeled 'Impact'. The diagonal axis from top-left to bottom-right is labeled 'Adj. Impact'. The diagonal axis from bottom-left to top-right is labeled 'Exploitability'. The bottom axis is labeled 'Temporal'. The left axis is labeled 'Environmental'. A blue dot at the center is labeled 'v3.1'.</p>	The context CVSS score chart is not available.

Table 39: CVE-2023-4813 Severity Charts**Rationale**

Score is below 7,0

Priority

Default	No elevated priority.
----------------	-----------------------

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2023-45853**Description**

MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. NOTE: MiniZip is not a supported part of the zlib product. NOTE: pyminizip through 0.2.6 is also vulnerable because it bundles an affected zlib version, and exposes the applicable MiniZip code through its compress API.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-45853

Table 40: CVE-2023-45853 References

Affected Components

Component	Artifact Id	Version
zlib	zlib-1.2.11	1.2.11

Table 41: CVE-2023-45853 Affected Components

Weakness

CWE-190

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Critical

Table 42: CVE-2023-45853 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	9.8	5.9	3.9

Table 43: CVE-2023-45853 Initial Severity Details

Advisories

Alerts

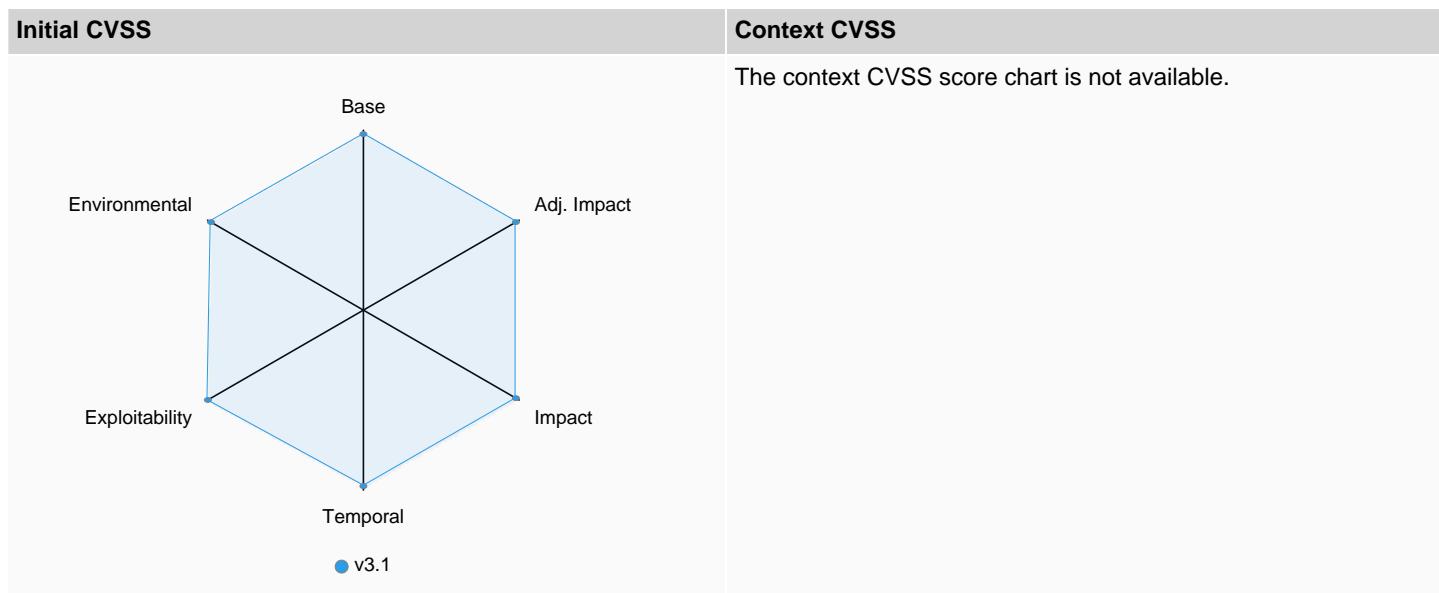
ID	Summary	Create Date	Update Date
GHSA-mq29-j5xf-cjwr	pyminizip affected by zlib's integer overflow/heap based buffer overflow vulnerability due to vulnerable dependency	2023-10-14	2023-10-14

Table 44: CVE-2023-45853 Alerts

Assessment

Summary

In Review
Default
Critical

**Table 45: CVE-2023-45853 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</code>
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2023-4527**Description**

A flaw was found in glibc. When the getaddrinfo function is called with the AF_UNSPEC address family and the system is configured with no-aaaa mode via /etc/resolv.conf, a DNS response via TCP larger than 2048 bytes can potentially disclose stack contents through the function returned address data, and may cause a crash.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-4527

Table 46: CVE-2023-4527 References**Affected Components**

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34

Component	Artifact Id	Version
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 47: CVE-2023-4527 Affected Components**Weakness**

CWE-125, CWE-121

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.5	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H	Medium

Table 48: CVE-2023-4527 Initial Severity

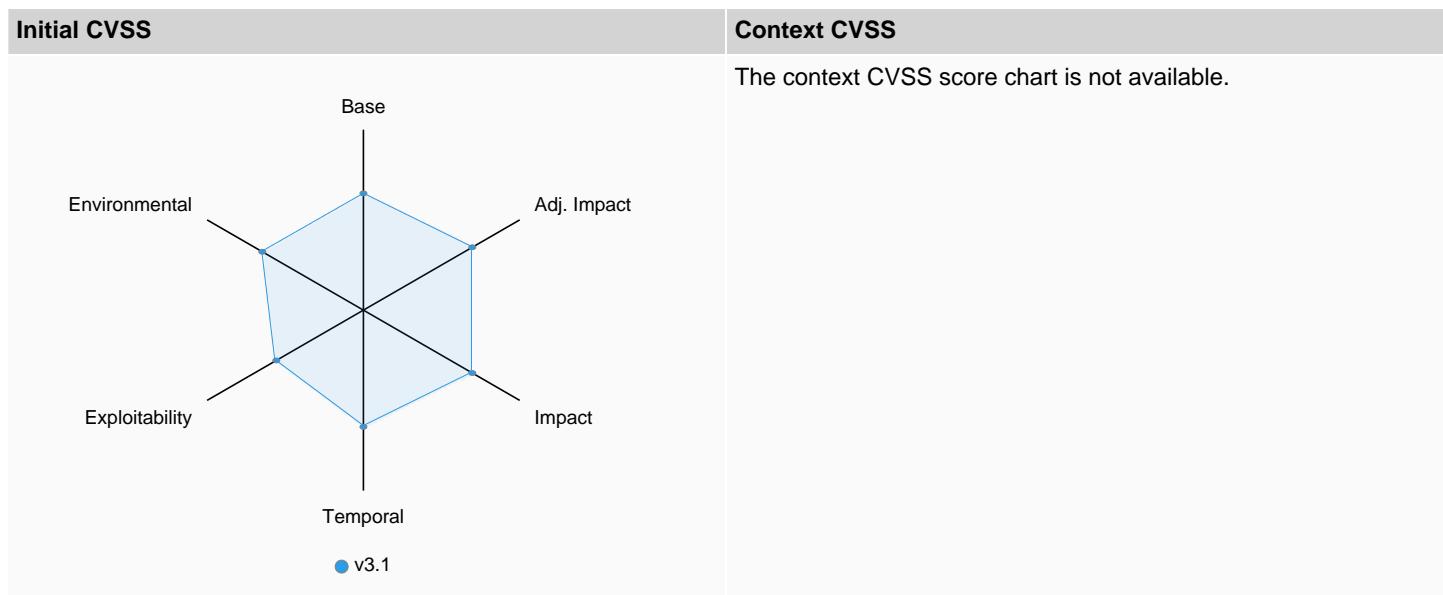
Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	6.5	4.2	2.2

Table 49: CVE-2023-4527 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-hmf7-f8gf-8f4p	A flaw was found in glibc. When the getaddrinfo function is called with the AF_UNSPEC address family and the system is configured with no-aaaa mode via /etc/resolv.conf, a DNS response via TCP larger than 2048 bytes can potentially disclose stack contents through the function returned address data, and may cause a crash.	2023-09-18	2023-09-18

Table 50: CVE-2023-4527 Alerts**Assessment****Summary**

Insignificant	Default	Medium
---------------	---------	--------

**Table 51: CVE-2023-4527 Severity Charts****Rationale**

Score is below 7,0

Priority

Default	No elevated priority.
----------------	-----------------------

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H</code>
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2023-4039**Description**

DISPUTED A failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-4039

Table 52: CVE-2023-4039 References

Affected Components

Component	Artifact Id	Version
libgcc	libgcc-11.4.1	11.4.1

Table 53: CVE-2023-4039 Affected Components

Weakness

CWE-693

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	4.8	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium

Table 54: CVE-2023-4039 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	4.8	2.5	2.2

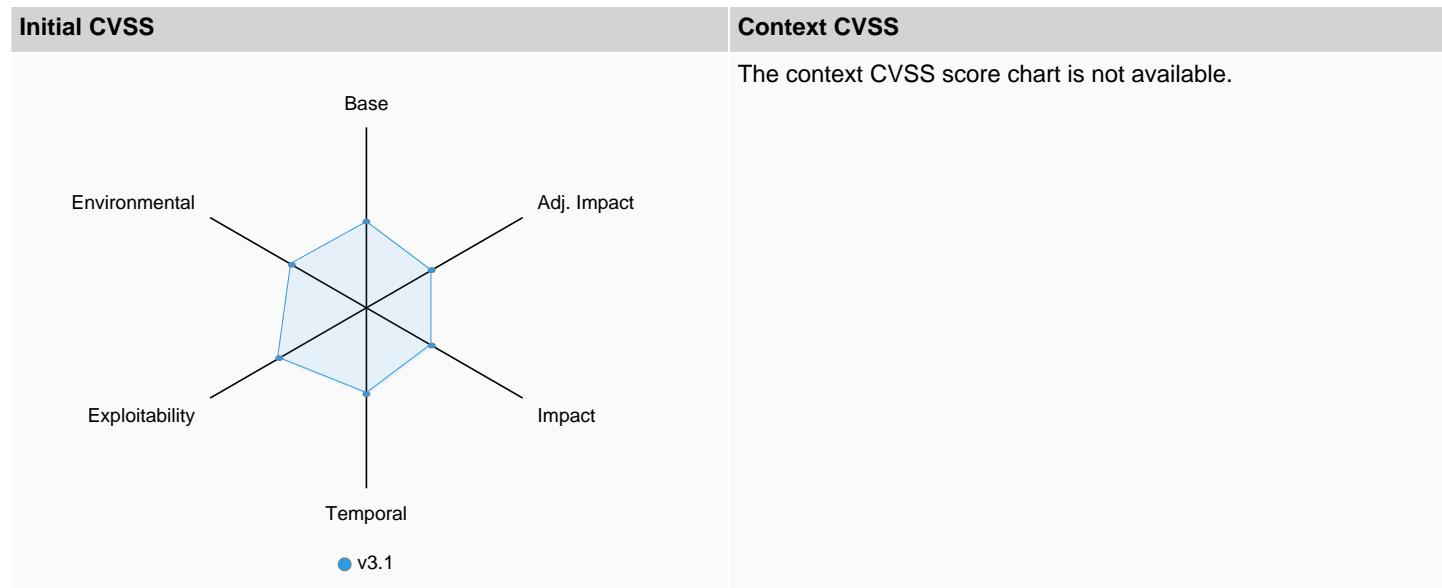
Table 55: CVE-2023-4039 Initial Severity Details

Advisories

No security advisories have been identified.

Assessment

Summary

Insignificant
Default
Medium
**Table 56: CVE-2023-4039 Severity Charts**

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2023-29491

Description

ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in \$HOME/.terminfo or reached via the TERMINFO or TERM environment variable.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-29491

Table 57: CVE-2023-29491 References

Affected Components

Component	Artifact Id	Version
ncurses-libs	ncurses-libs-6.2	6.2
ncurses-base	ncurses-base-6.2	6.2

Table 58: CVE-2023-29491 Affected Components

Weakness

CWE-787

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	High

Table 59: CVE-2023-29491 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.8	5.9	1.8

Table 60: CVE-2023-29491 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-vh2x-5rx6-qqhV	ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in \$HOME/.terminfo or reached via the TERMINFO or TERM environment variable.	2023-04-14	2023-04-14

Table 61: CVE-2023-29491 Alerts

Assessment

Summary

In Review Default High

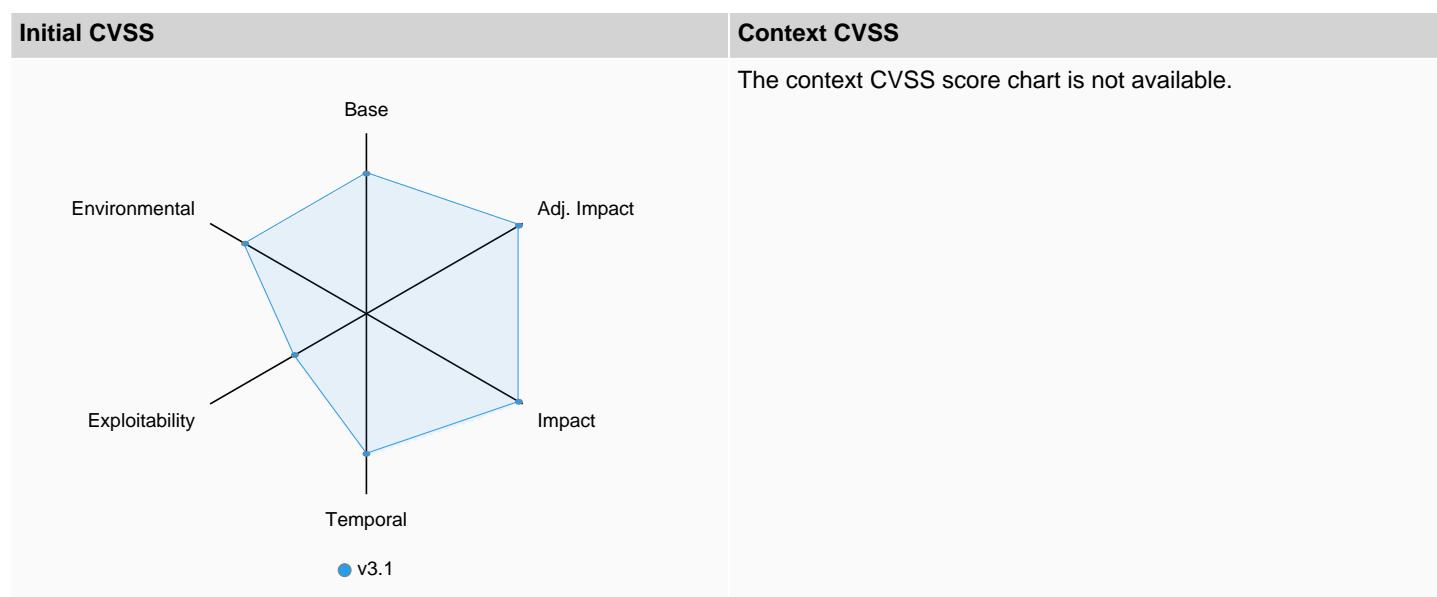


Table 62: CVE-2023-29491 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2023-2603

Description

A vulnerability was found in libcap. This issue occurs in the `_libcap_strdup()` function and can lead to an integer overflow if the input string is close to 4GiB.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-2603

Table 63: CVE-2023-2603 References

Affected Components

Component	Artifact Id	Version
libcap	libcap-2.48	2.48

Table 64: CVE-2023-2603 Affected Components

Weakness

CWE-190

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	High

Table 65: CVE-2023-2603 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.8	5.9	1.8

Table 66: CVE-2023-2603 Initial Severity Details

Advisories

Alerts

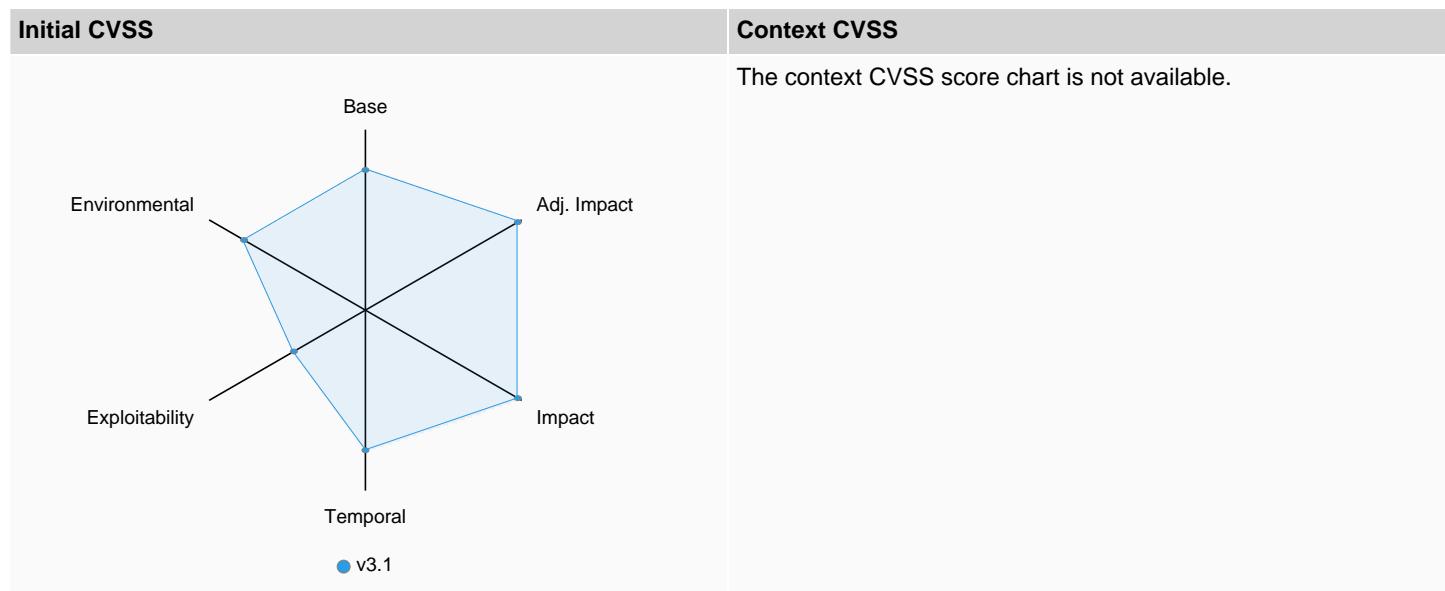
Id	Summary	Create Date	Update Date
GHSA-wp54-pwvg-rqq5	A vulnerability was found in libcap. This issue occurs in the <code>_libcap_strdup()</code> function and can lead to an integer overflow if the input string is close to 4GiB.	2023-06-06	2023-06-06

Table 67: CVE-2023-2603 Alerts

Assessment

Summary

In Review Default High

**Table 68: CVE-2023-2603 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</code>
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2023-0687**Description**

A vulnerability was found in GNU C Library 2.38. It has been declared as critical. This vulnerability affects the function `_monstartup` of the file `gmon.c` of the component Call Graph Monitor. The manipulation leads to buffer overflow. It is recommended to apply a patch to fix this issue. VDB-220246 is the identifier assigned to this vulnerability. NOTE: The real existence of this vulnerability is still doubted at the moment. The inputs that induce this vulnerability are basically addresses of the running application that is built with gmon enabled. It's basically trusted input or input that needs an actual security flaw to be compromised or controlled.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-0687

Table 69: CVE-2023-0687 References

Affected Components

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 70: CVE-2023-0687 Affected Components

Weakness

CWE-120

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Critical
CVSS:2.0	NVD-CNA-NVD	4.0	AV:A/AC:H/Au:S/C:P/I:P/A:P	Medium

Table 71: CVE-2023-0687 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	9.8	5.9	3.9
CVSS:2.0	NVD-CNA-NVD	4.0	6.4	2.5

Table 72: CVE-2023-0687 Initial Severity Details

Advisories

Alerts

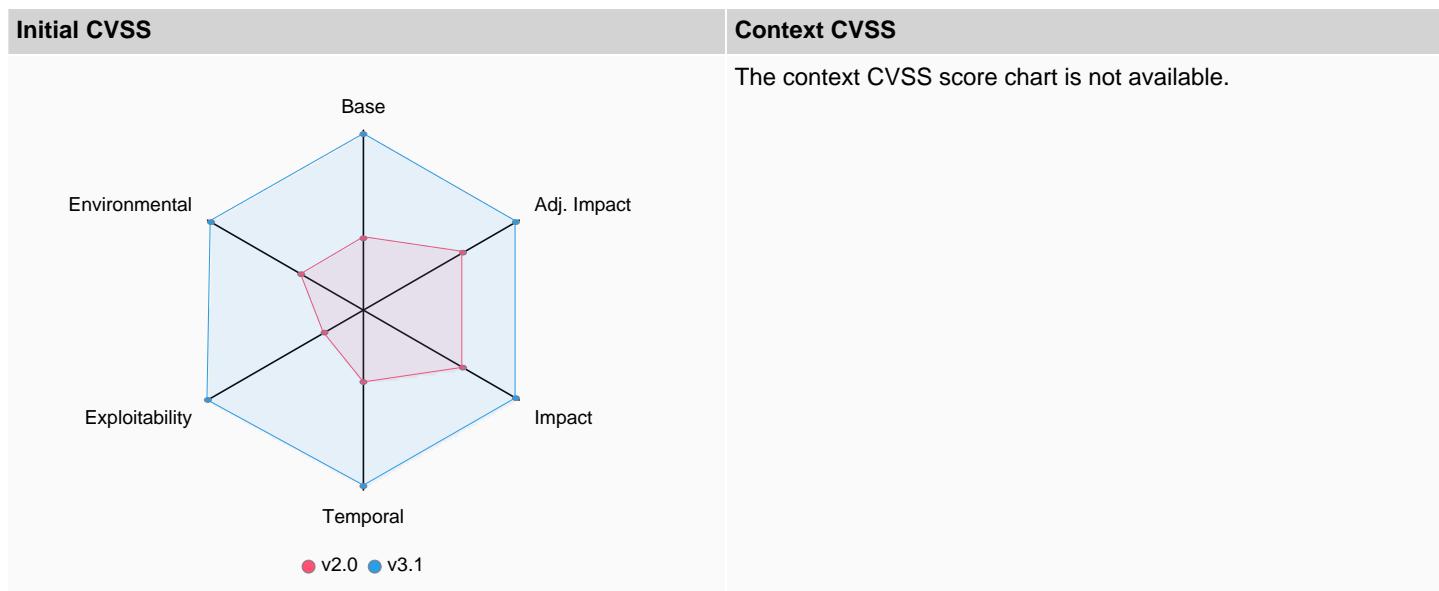
ID	Summary	Create Date	Update Date
GHSA-5r4p-4pqv-gqhw	A vulnerability was found in GNU C Library 2.38. It has been declared as critical. This vulnerability affects the function __monstartup of the file gmon.c of the component Call Graph Monitor. The manipulation leads to buffer overflow. It is recommended to apply a patch to fix this issue. VDB-220246 is the identifier assigned to this vulnerability.	2023-02-06	2023-02-06

Table 73: CVE-2023-0687 Alerts

Assessment

Summary

In Review Default Critical

**Table 74: CVE-2023-0687 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2022-41409**Description**

Integer overflow vulnerability in pcre2test before 10.41 allows attackers to cause a denial of service or other unspecified impacts via negative input.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-41409

Table 75: CVE-2022-41409 References**Affected Components**

Component	Artifact Id	Version
pcre2	pcre2-10.40	10.40

Component	Artifact Id	Version
pcre2-syntax	pcre2-syntax-10.40	10.40

Table 76: CVE-2022-41409 Affected Components**Weakness**

CWE-190

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	High

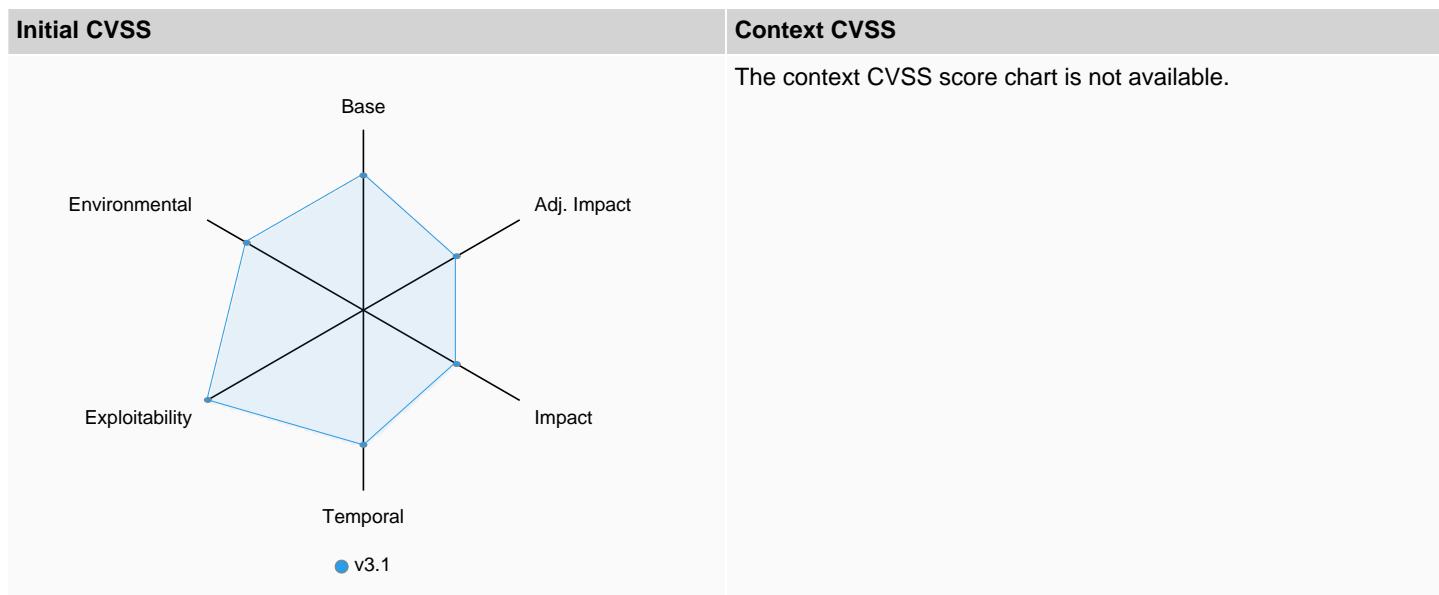
Table 77: CVE-2022-41409 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.5	3.6	3.9

Table 78: CVE-2022-41409 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-4qfx-v7wh-3q4j	Integer overflow vulnerability in pcre2test before 10.41 allows attackers to cause a denial of service or other unspecified impacts via negative input.	2023-07-18	2023-07-18

Table 79: CVE-2022-41409 Alerts**Assessment****Summary**
In Review
Due
High

**Table 80: CVE-2022-41409 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Due (8.5 from base score 7.5)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</code>
Keywords	resource exemption: An adversary may attempt to exhaust resources of the system compromising performance objectives and availability.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2022-37832**Description**

Mutiny 7.2.0-10788 suffers from Hardcoded root password.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-37832

Table 81: CVE-2022-37832 References**Affected Components**

Component	Artifact Id	Version
	io.quarkus.quarkus-mutiny-3.8.5.jar	3.8.5

Component	Artifact Id	Version
	io.quarkus.quarkus-mutiny-deployment-3.8.5.jar	3.8.5

Table 82: CVE-2022-37832 Affected Components**Weakness**

CWE-798

Initial Severity

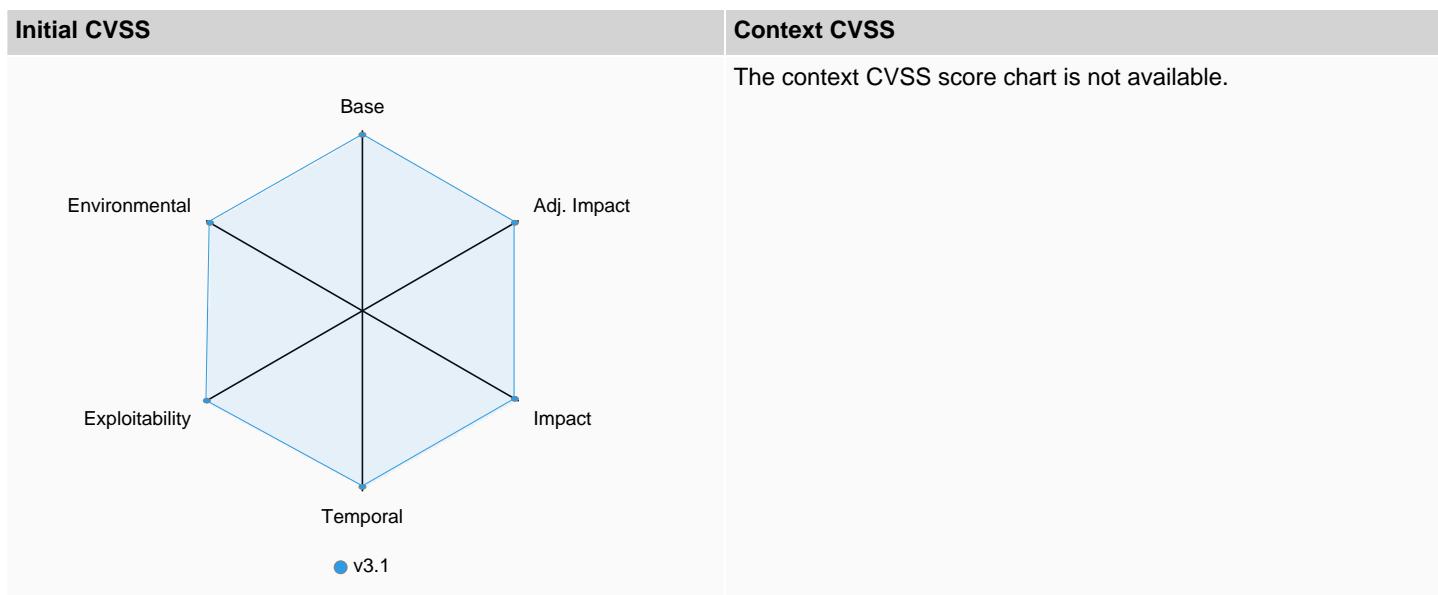
Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Critical

Table 83: CVE-2022-37832 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	9.8	5.9	3.9

Table 84: CVE-2022-37832 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-999r-r2f8-xm55	Mutiny 7.2.0-10788 suffers from Hardcoded root password.	2022-12-17	2022-12-17

Table 85: CVE-2022-37832 Alerts**Assessment****Summary**
In Review
Default
Critical
**Table 86: CVE-2022-37832 Severity Charts**

Rationale

The vulnerability has automatically been marked as in review.

Priority**Default**

No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2022-37434**Description**

zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference).

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-37434

Table 87: CVE-2022-37434 References**Affected Components**

Component	Artifact Id	Version
zlib	zlib-1.2.11	1.2.11

Table 88: CVE-2022-37434 Affected Components**Weakness**

CWE-787

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Critical

Table 89: CVE-2022-37434 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	9.8	5.9	3.9

Table 90: CVE-2022-37434 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-cfmr-vrgj-vqvw	zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference).	2022-08-06	2022-08-06

Table 91: CVE-2022-37434 Alerts

Assessment

Summary

In Review Default Critical

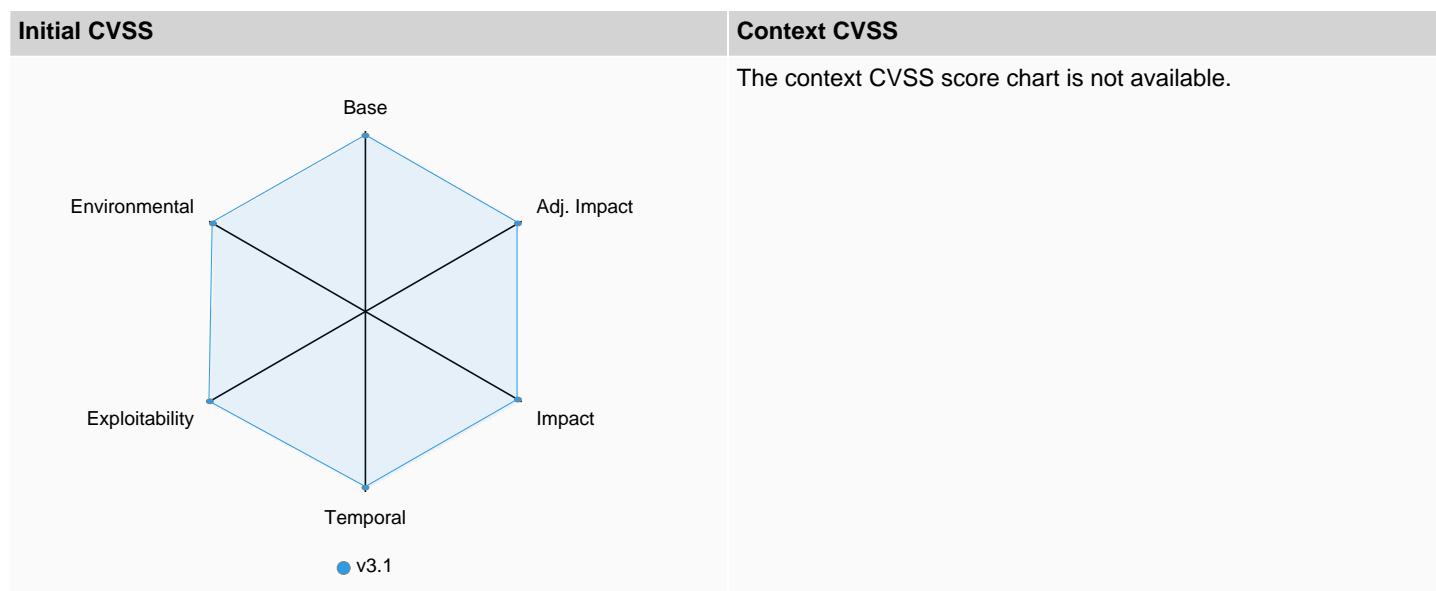


Table 92: CVE-2022-37434 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2022-35737

Description

SQLite 1.0.12 through 3.39.x before 3.39.2 sometimes allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-35737

Table 93: CVE-2022-35737 References

Affected Components

Component	Artifact Id	Version
sqlite-libs	sqlite-libs-3.34.1	3.34.1

Table 94: CVE-2022-35737 Affected Components

Weakness

CWE-129

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	High

Table 95: CVE-2022-35737 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.5	3.6	3.9

Table 96: CVE-2022-35737 Initial Severity Details

Advisories

Alerts

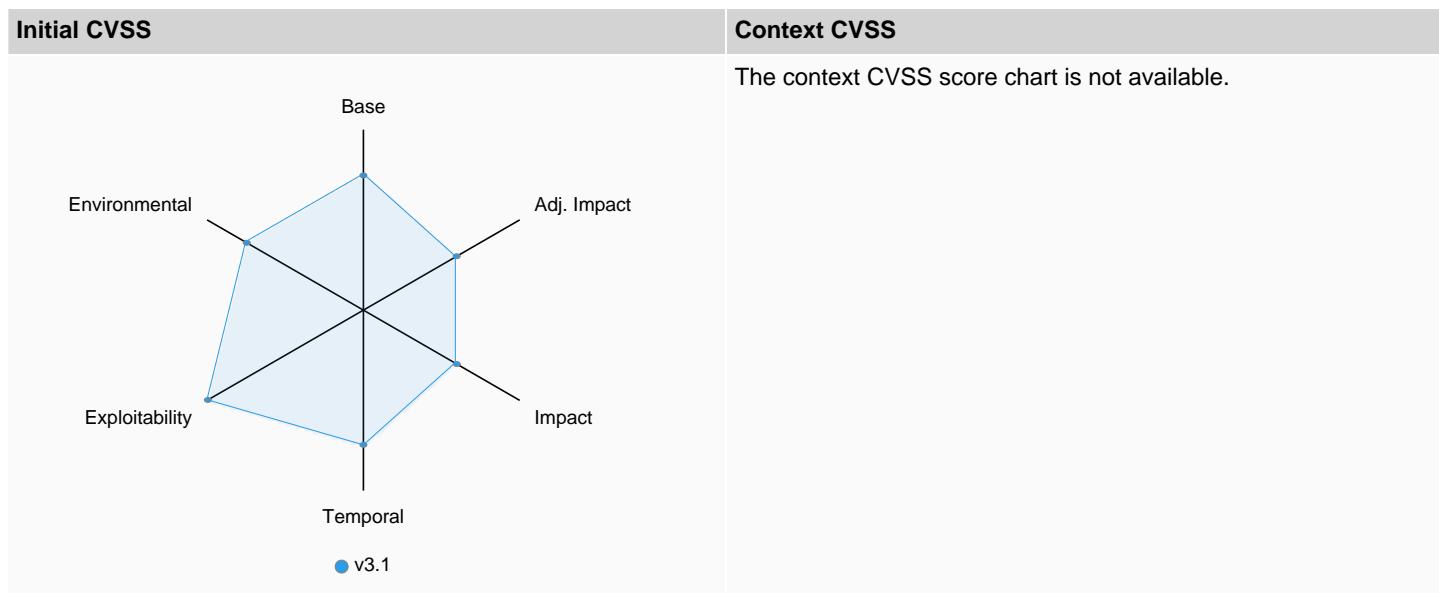
Id	Summary	Create Date	Update Date
GHSA-jw36-hf63-69r9	`libsqlite3-sys` via C SQLite improperly validates array index	2022-08-04	2022-08-04

Table 97: CVE-2022-35737 Alerts

Assessment

Summary

In Review	Default	High
-----------	---------	------

**Table 98: CVE-2022-35737 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</code>
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	<code>sqlite</code> (ver. 3) is still supported by its vendor. Support End Date: no date provided Vendor does not provide extended support for this product.

CVE-2022-29458**Description**

ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in tinfo/read_entry.c in the terminfo library.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-29458

Table 99: CVE-2022-29458 References**Affected Components**

Component	Artifact Id	Version
ncurses-libs	ncurses-libs-6.2	6.2

Component	Artifact Id	Version
ncurses-base	ncurses-base-6.2	6.2

Table 100: CVE-2022-29458 Affected Components**Weakness**

CWE-125

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.1	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H	High
CVSS:2.0	NVD-CNA-NVD	5.8	AV:N/AC:M/Au:N/C:P/I:N/A:P	Medium

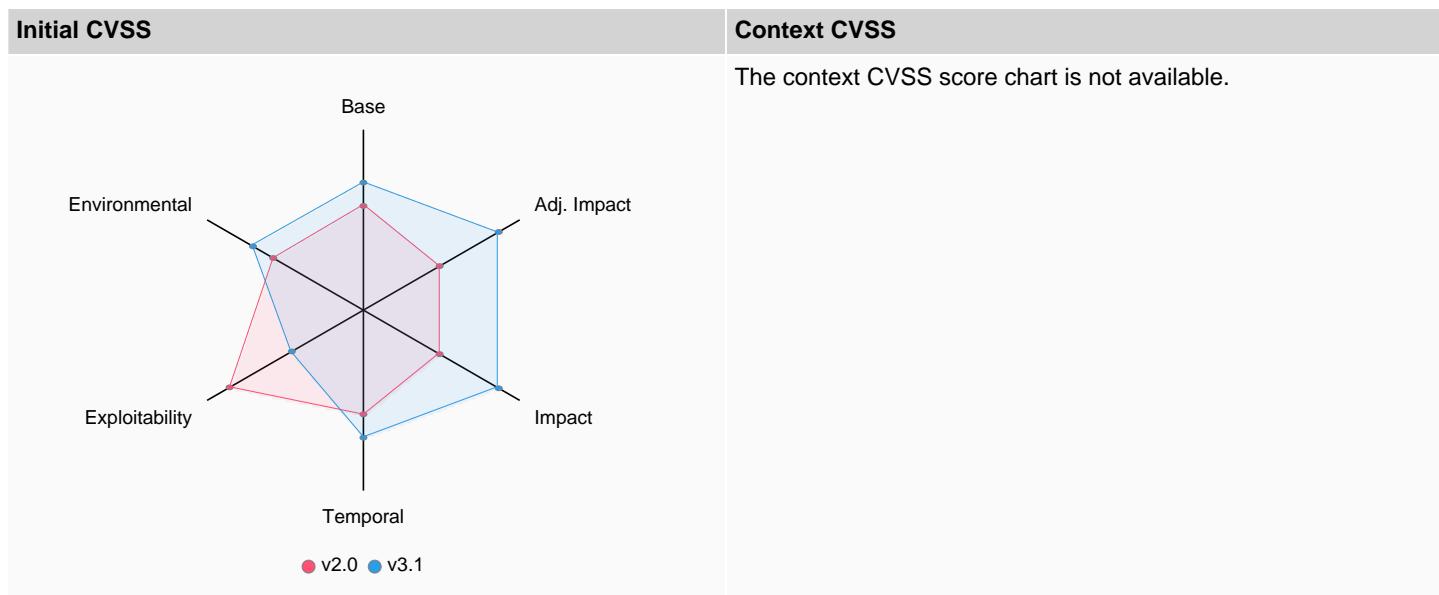
Table 101: CVE-2022-29458 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.1	5.2	1.8
CVSS:2.0	NVD-CNA-NVD	5.8	4.9	8.6

Table 102: CVE-2022-29458 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-jh4f-5j2m-4v9c	ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in tinfo/read_entry.c in the terminfo library.	2022-04-19	2022-04-19

Table 103: CVE-2022-29458 Alerts**Assessment****Summary**
In Review
Default
High

**Table 104: CVE-2022-29458 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H</code>
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2022-23219**Description**

The deprecated compatibility function `clnt_create` in the `sunrpc` module of the GNU C Library (aka glibc) through 2.34 copies its `hostname` argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-23219

Table 105: CVE-2022-23219 References**Affected Components**

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34

Component	Artifact Id	Version
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 106: CVE-2022-23219 Affected Components**Weakness**

CWE-120

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Critical
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Table 107: CVE-2022-23219 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	9.8	5.9	3.9
CVSS:2.0	NVD-CNA-NVD	7.5	6.4	10.0

Table 108: CVE-2022-23219 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-fhxm-4mc9-6jf5	The deprecated compatibility function clnt_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its hostname argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.	2022-01-15	2022-01-15

Table 109: CVE-2022-23219 Alerts**Assessment****Summary**
In Review
Escalate
Critical

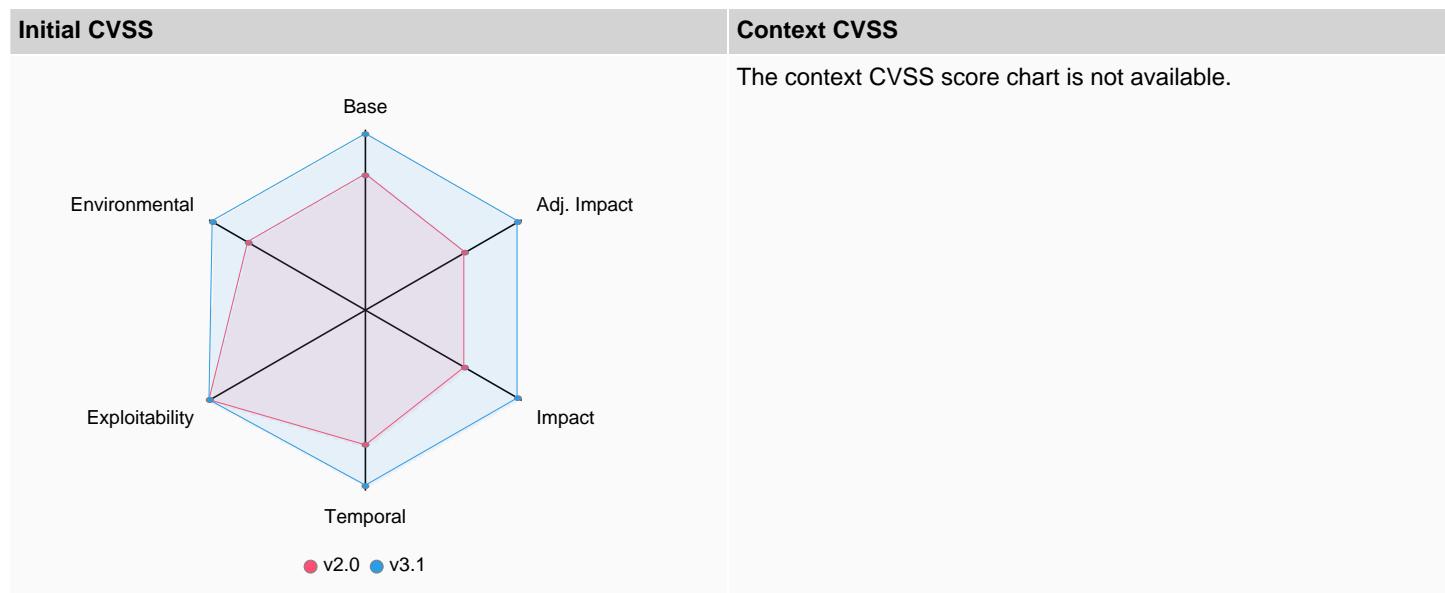


Table 110: CVE-2022-23219 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (13.8 from base score 9.8)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	privilege escalation: An adversary may gain further privileges and gain unauthorized access to the system or services. resource exemption: An adversary may attempt to exhaust resources of the system compromising performance objectives and availability.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2022-23218

Description

The deprecated compatibility function `svcupnix_create` in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its path argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-23218

Table 111: CVE-2022-23218 References

Affected Components

Component	Artifact Id	Version
glibc	glibc-2.34	2.34

Component	Artifact Id	Version
glibc-common	glibc-common-2.34	2.34
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 112: CVE-2022-23218 Affected Components**Weakness**

CWE-120

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Critical
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

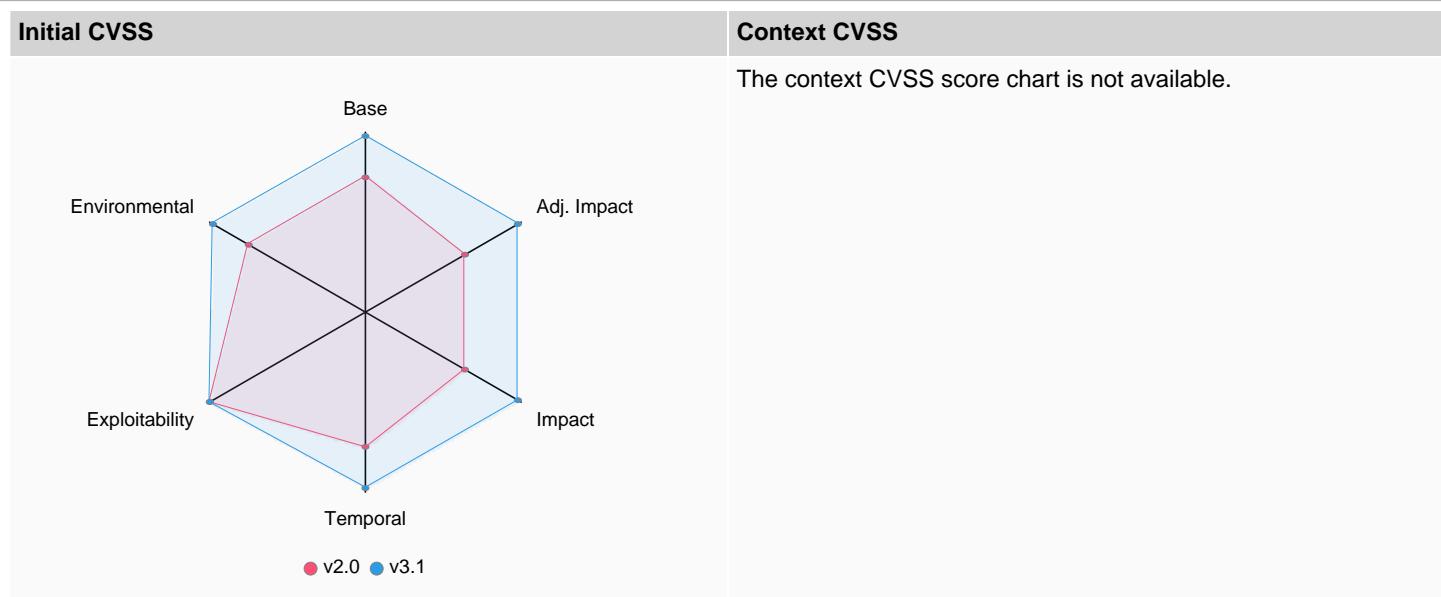
Table 113: CVE-2022-23218 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	9.8	5.9	3.9
CVSS:2.0	NVD-CNA-NVD	7.5	6.4	10.0

Table 114: CVE-2022-23218 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-8g8v-256r-57v7	The deprecated compatibility function svcunix_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its path argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.	2022-01-15	2022-01-15

Table 115: CVE-2022-23218 Alerts**Assessment****Summary**
In Review
Escalate
Critical

**Table 116: CVE-2022-23218 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Escalate (13.8 from base score 9.8)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</code>
Keywords	privilege escalation: An adversary may gain further privileges and gain unauthorized access to the system or services. resource exemption: An adversary may attempt to exhaust resources of the system compromising performance objectives and availability.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2021-46848**Description**

GNU Libtasn1 before 4.19.0 has an ETYPENOK off-by-one array size check that affects asn1_encode_simple_der.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-46848

Table 117: CVE-2021-46848 References**Affected Components**

Component	Artifact Id	Version
libtasn1	libtasn1-4.16.0	4.16.0

Table 118: CVE-2021-46848 Affected Components

Weakness

CWE-193

Initial Severity

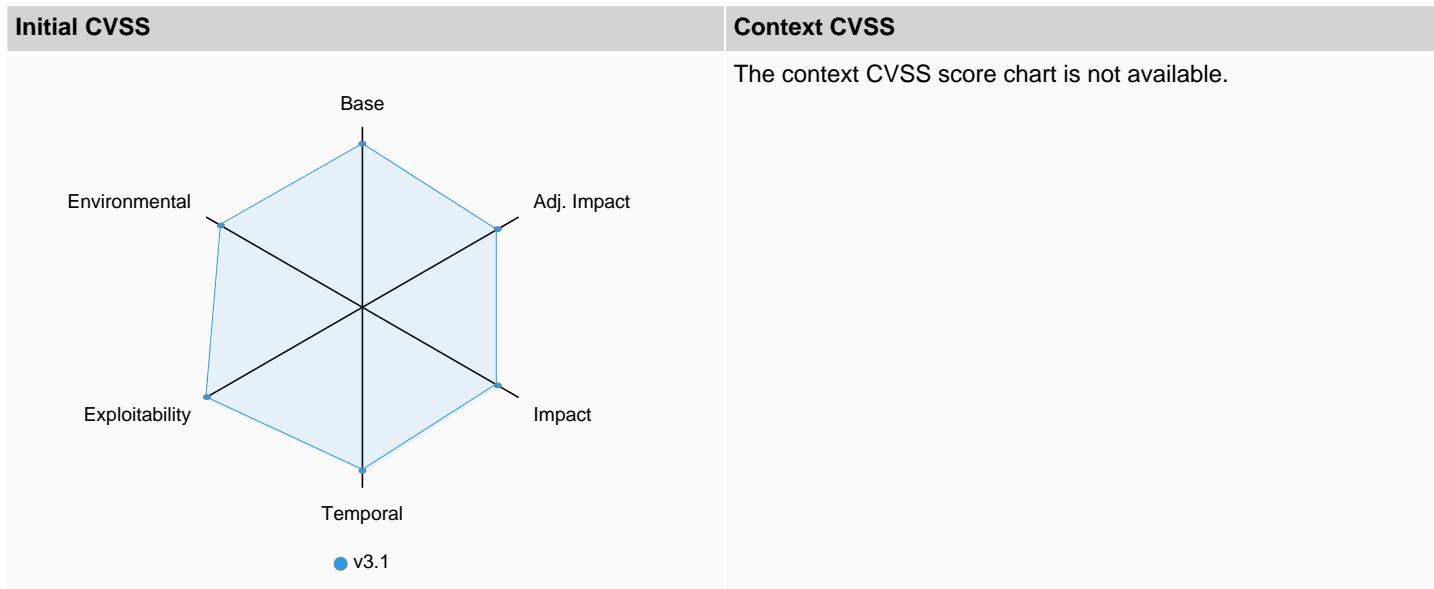
Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H	Critical

Table 119: CVE-2021-46848 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	9.1	5.2	3.9

Table 120: CVE-2021-46848 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-6468-68pw-9chw	GNU Libtasn1 before 4.19.0 has an ETYPE_OK off-by-one array size check that affects asn1_encode_simple_der.	2022-10-24	2022-10-24

Table 121: CVE-2021-46848 Alerts**Assessment****Summary**
In Review
Default
Critical
**Table 122: CVE-2021-46848 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2021-43396

Description

In `iconvdata/iso-2022-jp-3.c` in the GNU C Library (aka glibc) 2.34, remote attackers can force `iconv()` to emit a spurious '\0' character via crafted ISO-2022-JP-3 data that is accompanied by an internal state reset. This may affect data integrity in certain `iconv()` use cases. NOTE: the vendor states "the bug cannot be invoked through user input and requires `iconv` to be invoked with a NULL inbuf, which ought to require a separate application bug to do so unintentionally. Hence there's no security impact to the bug."

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-43396

Table 123: CVE-2021-43396 References

Affected Components

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 124: CVE-2021-43396 Affected Components

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	High
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium

Table 125: CVE-2021-43396 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.5	3.6	3.9
CVSS:2.0	NVD-CNA-NVD	5.0	2.9	10.0

Table 126: CVE-2021-43396 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-73g2-m4v3-6c2h	In iconvdata/iso-2022-jp-3.c in the GNU C Library (aka glibc) 2.34, remote attackers can force iconv() to emit a spurious '\0' character via crafted ISO-2022-JP-3 data that is accompanied by an internal state reset. This may affect data integrity in certain iconv() use cases.	2022-05-24	2022-05-24

Table 127: CVE-2021-43396 Alerts

Assessment

Summary

In Review Escalate High

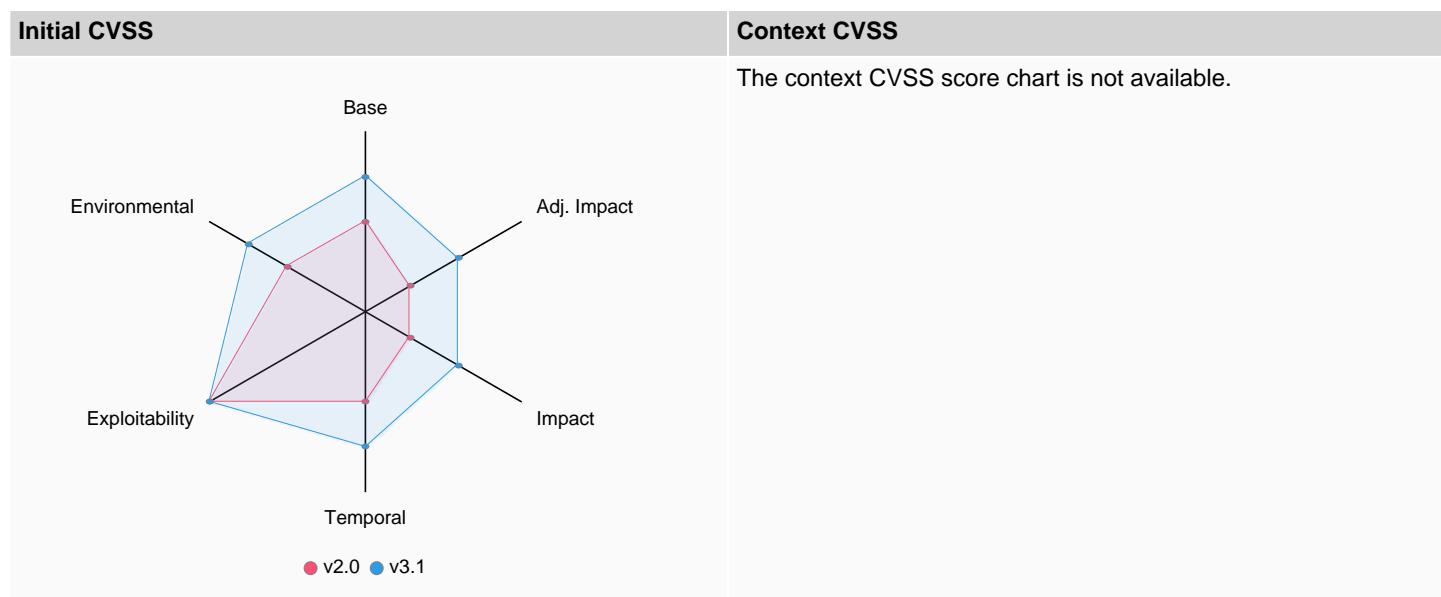


Table 128: CVE-2021-43396 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (10.5 from base score 7.5)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Keywords	external attacker: An adversary may attempt to attack the system from remote. The adversary may modify / reconfigure existing code or introduce code from remote.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2021-3998

Description

A flaw was found in glibc. The realpath() function can mistakenly return an unexpected value, potentially leading to information leakage and disclosure of sensitive data.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-3998

Table 129: CVE-2021-3998 References

Affected Components

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 130: CVE-2021-3998 Affected Components

Weakness

CWE-125, CWE-252

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	High

Table 131: CVE-2021-3998 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.5	3.6	3.9

Table 132: CVE-2021-3998 Initial Severity Details

Advisories

Alerts

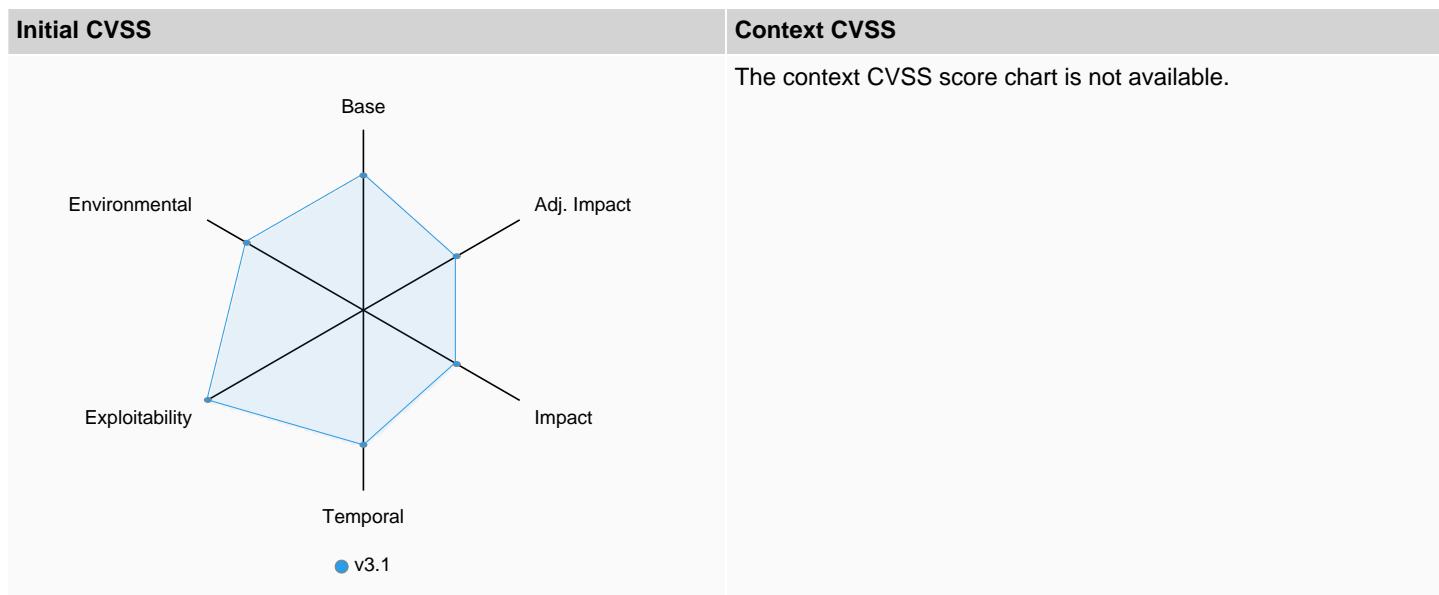
Id	Summary	Create Date	Update Date
GHSA-32pr-wg5j-9rwr	A flaw was found in glibc. The realpath() function can mistakenly return an unexpected value, potentially leading to information leakage and disclosure of sensitive data.	2022-08-25	2022-08-25

Table 133: CVE-2021-3998 Alerts

Assessment

Summary

In Review Default High

**Table 134: CVE-2021-3998 Severity Charts****Rationale**

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N</code>
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2021-39537**Description**

An issue was discovered in ncurses through v6.2-1. `_nc_captainfo` in `captainfo.c` has a heap-based buffer overflow.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-39537

Table 135: CVE-2021-39537 References**Affected Components**

Component	Artifact Id	Version
ncurses-libs	ncurses-libs-6.2	6.2
ncurses-base	ncurses-base-6.2	6.2

Table 136: CVE-2021-39537 Affected Components

Weakness

CWE-787

Initial Severity

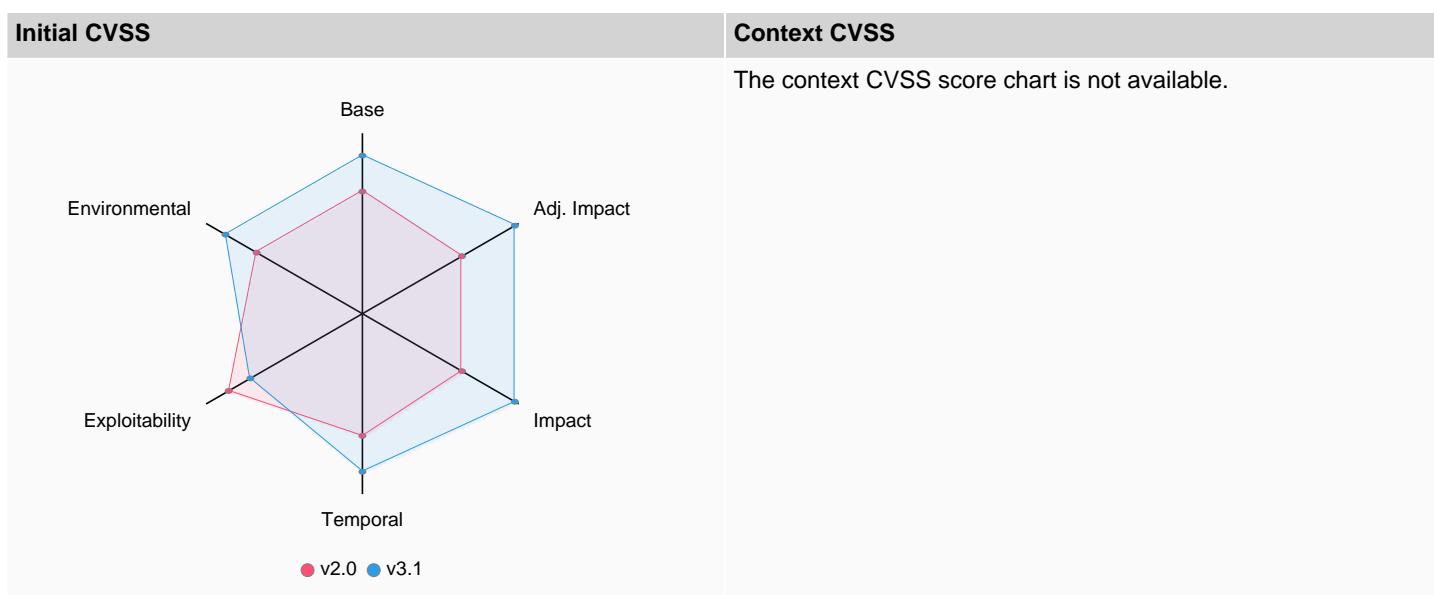
Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	8.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	High
CVSS:2.0	NVD-CNA-NVD	6.8	AV:N/AC:M/Au:N/C:P/I:P/A:P	Medium

Table 137: CVE-2021-39537 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	8.8	5.9	2.8
CVSS:2.0	NVD-CNA-NVD	6.8	6.4	8.6

Table 138: CVE-2021-39537 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-v5gv-3mwr-6223	An issue was discovered in ncurses through v6.2-1. _nc_captainfo in captaininfo.c has a heap-based buffer overflow.	2022-05-24	2022-05-24

Table 139: CVE-2021-39537 Alerts**Assessment****Summary**
In Review
Default
High
**Table 140: CVE-2021-39537 Severity Charts**

Rationale

The vulnerability has automatically been marked as in review.

Priority**Default**

No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2021-38604**Description**

In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-38604

Table 141: CVE-2021-38604 References**Affected Components**

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 142: CVE-2021-38604 Affected Components**Weakness**

CWE-476

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	High
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Table 143: CVE-2021-38604 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.5	3.6	3.9

Scheme	Source	Base	Impact	Exploitability
CVSS:2.0	NVD-CNA-NVD	5.0	2.9	10.0

Table 144: CVE-2021-38604 Initial Severity Details

Advisories

Alerts

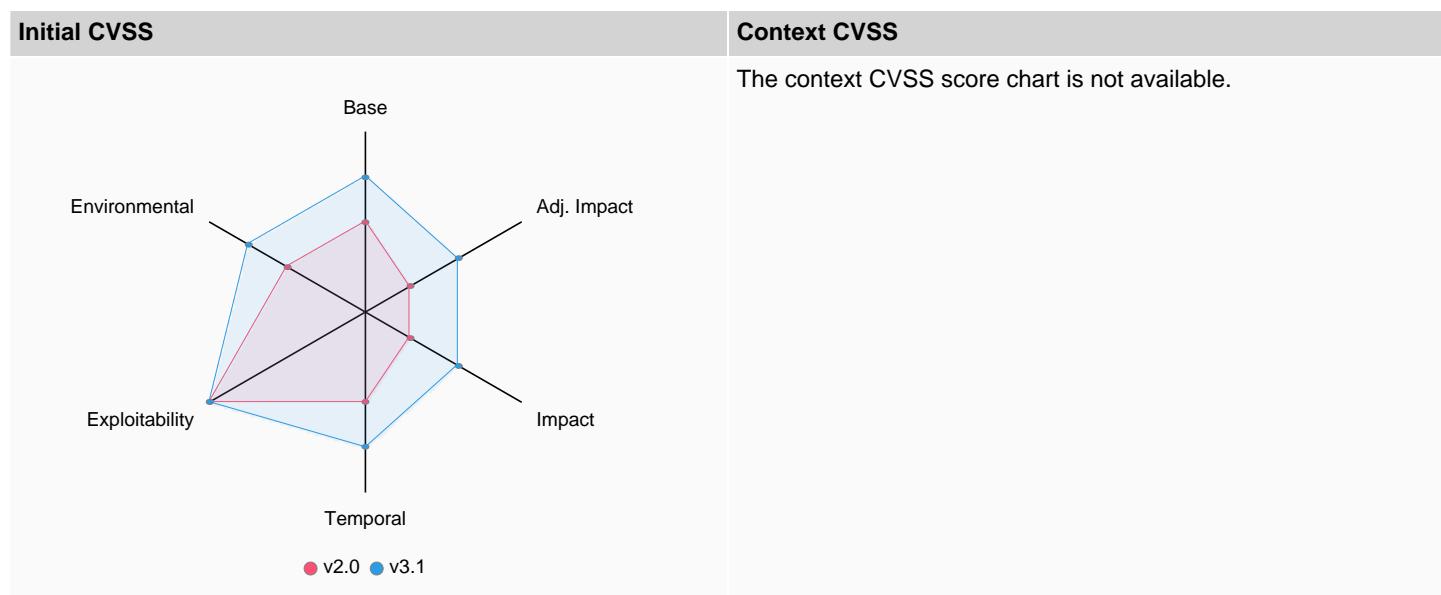
Id	Summary	Create Date	Update Date
GHSA-p3v7-wjmc-7fh8	In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.	2022-05-24	2022-05-24

Table 145: CVE-2021-38604 Alerts

Assessment

Summary

In Review Default High

**Table 146: CVE-2021-38604 Severity Charts**

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.

Criteria	Explanation
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2020-25638

Description

A flaw was found in hibernate-core in versions prior to and including 5.4.23.Final. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SQL comments of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. The highest threat from this vulnerability is to data confidentiality and integrity.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-25638

Table 147: CVE-2020-25638 References

Affected Components

Component	Artifact Id	Version
	io.quarkus.quarkus-hibernate-orm-3.8.5.jar	3.8.5
	io.quarkus.quarkus-hibernate-orm-deployment-3.8.5.jar	3.8.5
	io.quarkus.quarkus-hibernate-orm-deployment-spi-3.8.5.jar	3.8.5

Table 148: CVE-2020-25638 Affected Components

Weakness

CWE-89

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.4	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N	High
CVSS:2.0	NVD-CNA-NVD	5.8	AV:N/AC:M/Au:N/C:P/I:P/A:N	Medium

Table 149: CVE-2020-25638 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.4	5.2	2.2
CVSS:2.0	NVD-CNA-NVD	5.8	4.9	8.6

Table 150: CVE-2020-25638 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-j8jw-g6fq-mp7h	SQL injection in hibernate-core	2022-02-09	2022-02-09

Table 151: CVE-2020-25638 Alerts

Assessment

Summary

In Review Escalate High

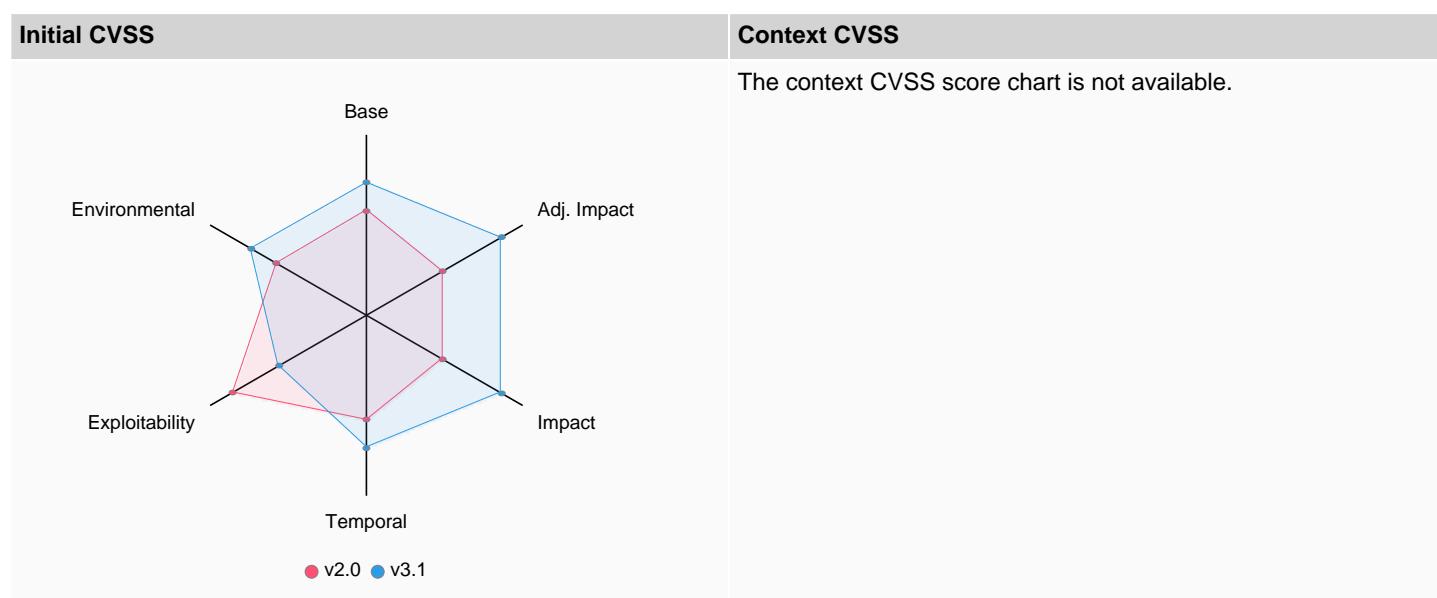


Table 152: CVE-2020-25638 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (10.4 from base score 7.4)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
Keywords	malicious content: An adversary may attempt to inject executable code or drafted messages to destabilize or compromise the system.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2020-13956

Description

Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URLs passed to the library as java.net.URI object and pick the wrong target host for request execution.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-13956

Table 153: CVE-2020-13956 References

Affected Components

Component	Artifact Id	Version
	org.apache.httpcomponents.httpcore-4.4.16.jar	4.4.16

Table 154: CVE-2020-13956 Affected Components

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium

Table 155: CVE-2020-13956 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	5.3	1.4	3.9
CVSS:2.0	NVD-CNA-NVD	5.0	2.9	10.0

Table 156: CVE-2020-13956 Initial Severity Details

Advisories

Alerts

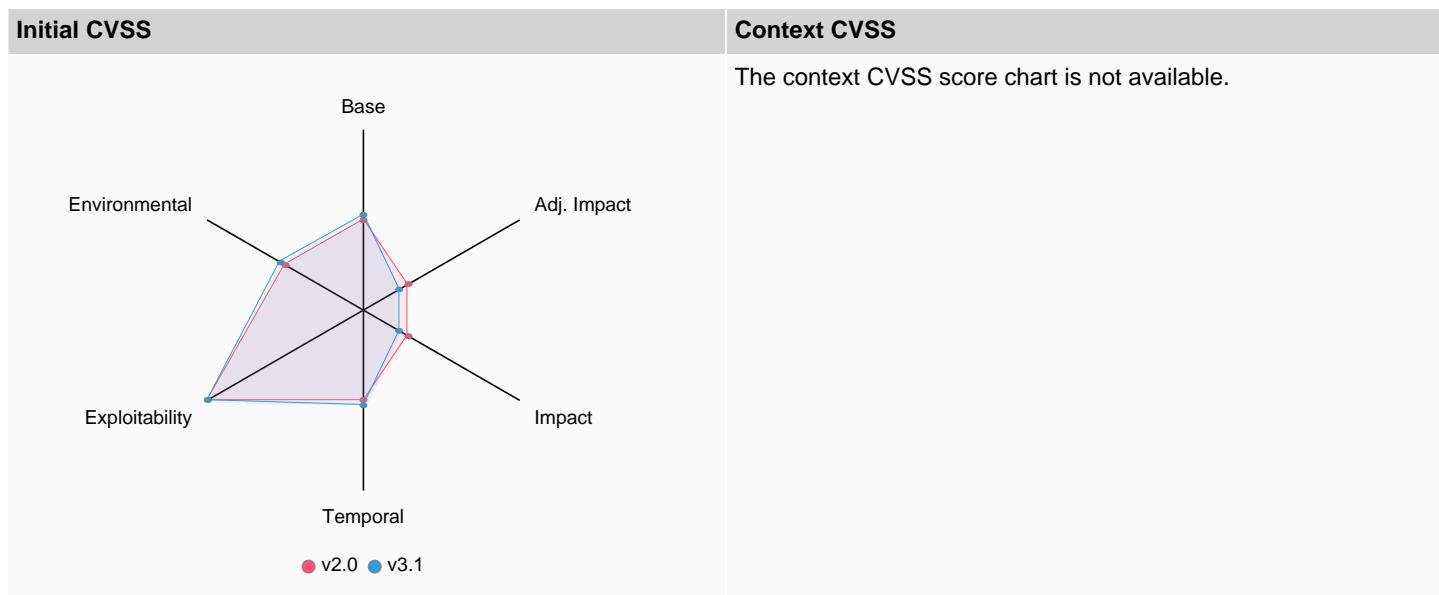
ID	Summary	Create Date	Update Date
GHSA-7r82-7xv7-xcpj	Cross-site scripting in Apache HttpClient	2021-06-03	2021-06-03

Table 157: CVE-2020-13956 Alerts

Assessment

Summary

Insignificant	Default	Medium
---------------	---------	--------

**Table 158: CVE-2020-13956 Severity Charts****Rationale**

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N</code>
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2019-14900**Description**

A flaw was found in Hibernate ORM in versions before 5.3.18, 5.4.18 and 5.5.0.Beta1. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SELECT or GROUP BY parts of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-14900

Table 159: CVE-2019-14900 References**Affected Components**

Component	Artifact Id	Version
	io.quarkus.quarkus-hibernate-orm-3.8.5.jar	3.8.5
	io.quarkus.quarkus-hibernate-orm-deployment-3.8.5.jar	3.8.5

Component	Artifact Id	Version
	io.quarkus.quarkus-hibernate-orm-deployment-spi-3.8.5.jar	3.8.5

Table 160: CVE-2019-14900 Affected Components**Weakness**

CWE-89

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.5	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	4.0	AV:N/AC:L/Au:S/C:P/I:N/A:N	Medium

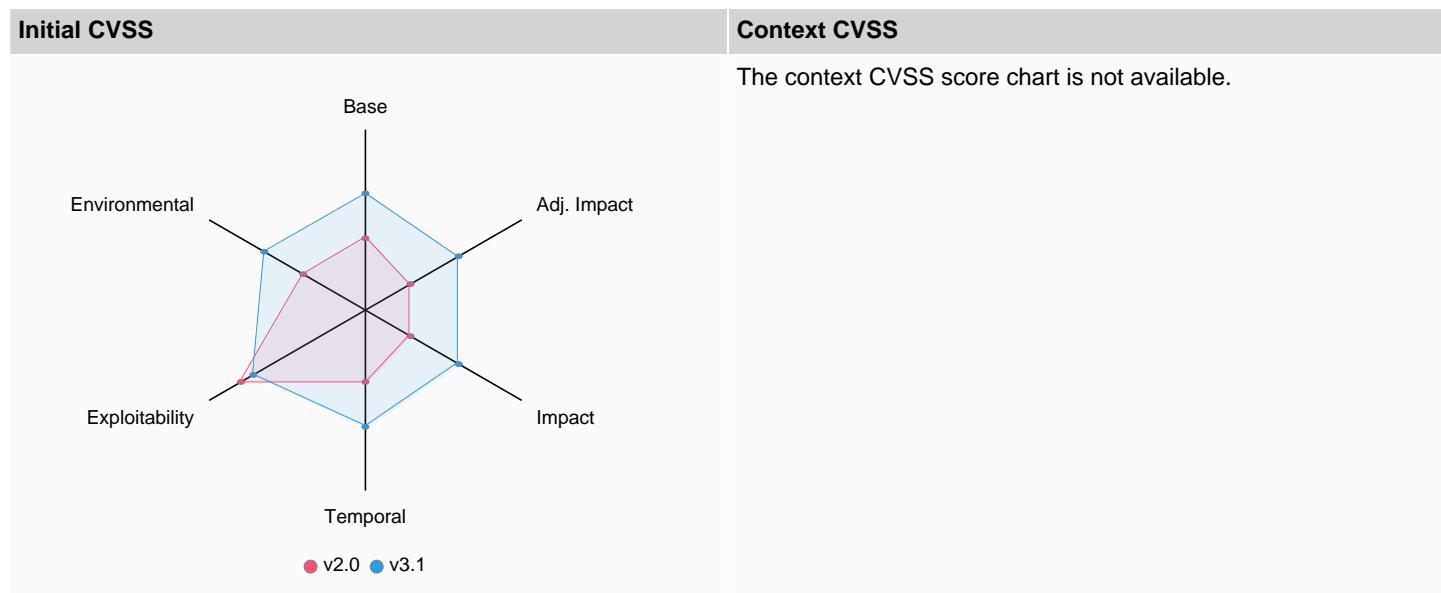
Table 161: CVE-2019-14900 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	6.5	3.6	2.8
CVSS:2.0	NVD-CNA-NVD	4.0	2.9	8.0

Table 162: CVE-2019-14900 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-8grg-q944-cch5	SQL Injection in Hibernate ORM	2022-02-10	2022-02-10

Table 163: CVE-2019-14900 Alerts**Assessment****Summary**
Insignificant
Escalate
Medium

**Table 164: CVE-2019-14900 Severity Charts****Rationale**

Score is below 7,0

Priority**Escalate** (9.5 from base score 6.5)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <code>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N</code>
Keywords	malicious content: An adversary may attempt to inject executable code or drafted messages to destabilize or compromise the system.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2018-25032**Description**

zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-25032

Table 165: CVE-2018-25032 References**Affected Components**

Component	Artifact Id	Version
zlib	zlib-1.2.11	1.2.11

Table 166: CVE-2018-25032 Affected Components

Weakness

CWE-787

Initial Severity

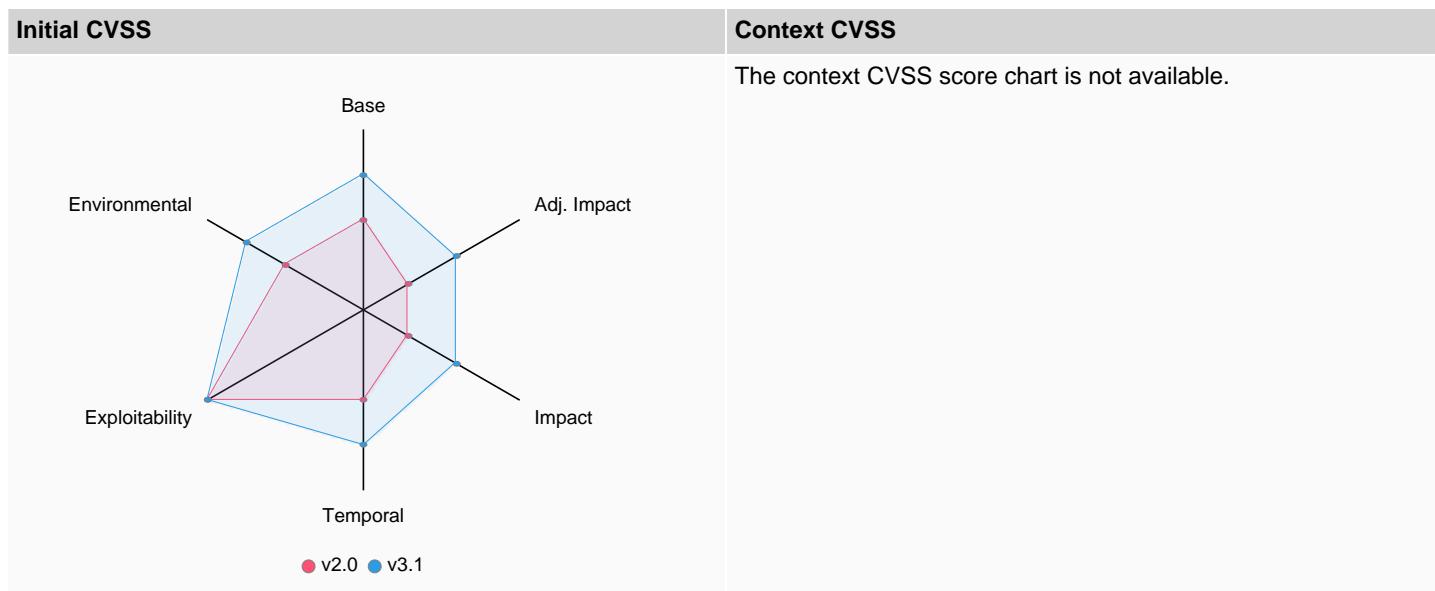
Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	High
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Table 167: CVE-2018-25032 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	7.5	3.6	3.9
CVSS:2.0	NVD-CNA-NVD	5.0	2.9	10.0

Table 168: CVE-2018-25032 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-jc36-42cf-vqwj	Nokogiri affected by zlib's Out-of-bounds Write vulnerability	2022-03-26	2022-03-26

Table 169: CVE-2018-25032 Alerts**Assessment****Summary**
In Review
Default
High
**Table 170: CVE-2018-25032 Severity Charts**

Rationale

The vulnerability has automatically been marked as in review.

Priority**Default**

No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2018-15529**Description**

A command injection vulnerability in maintenance.cgi in Mutiny "Monitoring Appliance" before 6.1.0-5263 allows authenticated users, with access to the admin interface, to inject arbitrary commands within the filename of a system upgrade upload.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-15529

Table 171: CVE-2018-15529 References**Affected Components**

Component	Artifact Id	Version
	io.quarkus.quarkus-mutiny-3.8.5.jar	3.8.5
	io.quarkus.quarkus-mutiny-deployment-3.8.5.jar	3.8.5

Table 172: CVE-2018-15529 Affected Components**Weakness**

CWE-78

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	High
CVSS:2.0	NVD-CNA-NVD	6.5	AV:N/AC:L/Au:S/C:P/I:P/A:P	Medium

Table 173: CVE-2018-15529 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	8.8	5.9	2.8

Scheme	Source	Base	Impact	Exploitability
CVSS:2.0	NVD-CNA-NVD	6.5	6.4	8.0

Table 174: CVE-2018-15529 Initial Severity Details

Advisories

Alerts

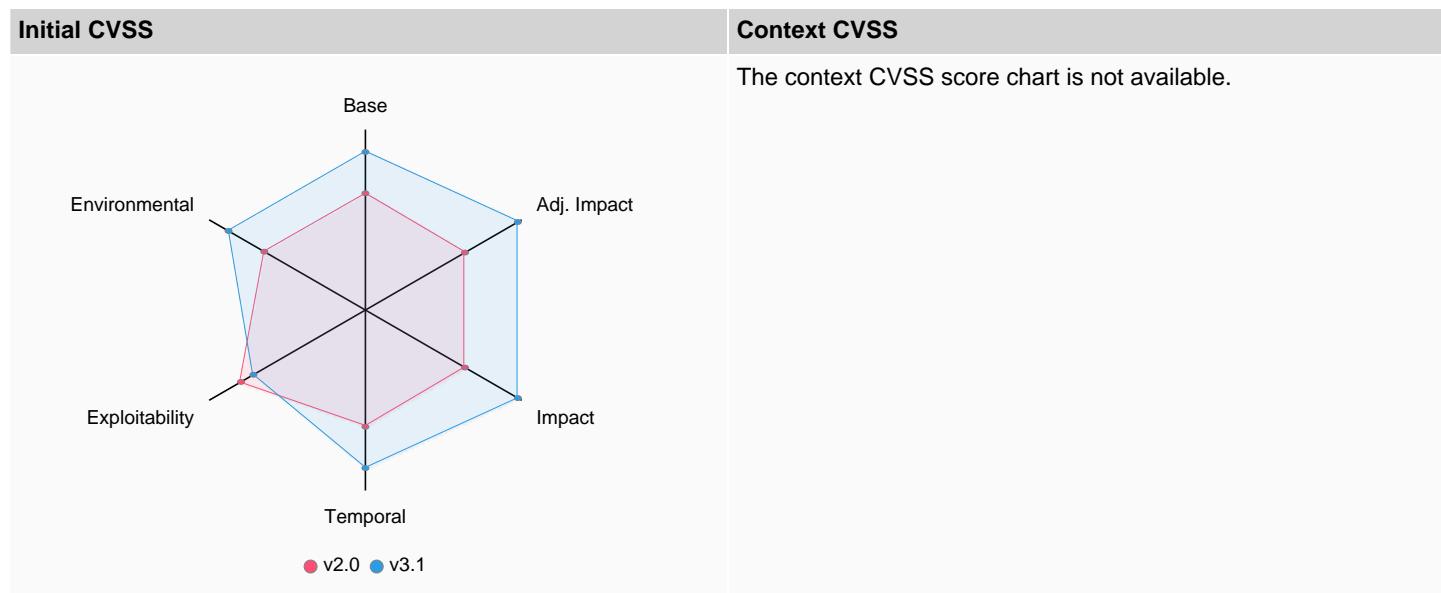
Id	Summary	Create Date	Update Date
GHSA-9xfc-48qq-9whq	A command injection vulnerability in maintenance.cgi in Mutiny "Monitoring Appliance" before 6.1.0-5263 allows authenticated users, with access to the admin interface, to inject arbitrary commands within the filename of a system upgrade upload.	2022-05-13	2022-05-13

Table 175: CVE-2018-15529 Alerts

Assessment

Summary

In Review Default High

**Table 176: CVE-2018-15529 Severity Charts**

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	No EPSS score available.

Criteria	Explanation
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2016-7091

Description

sudo: It was discovered that the default sudo configuration on Red Hat Enterprise Linux and possibly other Linux implementations preserves the value of INPUTRC which could lead to information disclosure. A local user with sudo access to a restricted program that uses readline could use this flaw to read content from specially formatted files with elevated privileges provided by sudo.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2016-7091

Table 177: CVE-2016-7091 References

Affected Components

Component	Artifact Id	Version
redhat-release	redhat-release-9.4	9.4

Table 178: CVE-2016-7091 Affected Components

Weakness

CWE-200

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	4.4	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	4.9	AV:L/AC:L/Au:N/C:C/I:N/A:N	Medium

Table 179: CVE-2016-7091 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	4.4	3.6	0.8
CVSS:2.0	NVD-CNA-NVD	4.9	6.9	3.9

Table 180: CVE-2016-7091 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-4h4j-rqc9-6rq3	sudo: It was discovered that the default sudo configuration on Red Hat Enterprise Linux and possibly other Linux implementations preserves the value of INPUTRC which could lead to information disclosure. A local user with sudo access to a restricted program that uses readline could use this flaw to read content from specially formatted files with elevated privileges provided by sudo.	2022-05-17	2022-05-17

Table 181: CVE-2016-7091 Alerts

Assessment

Summary

Insignificant Elevated Medium

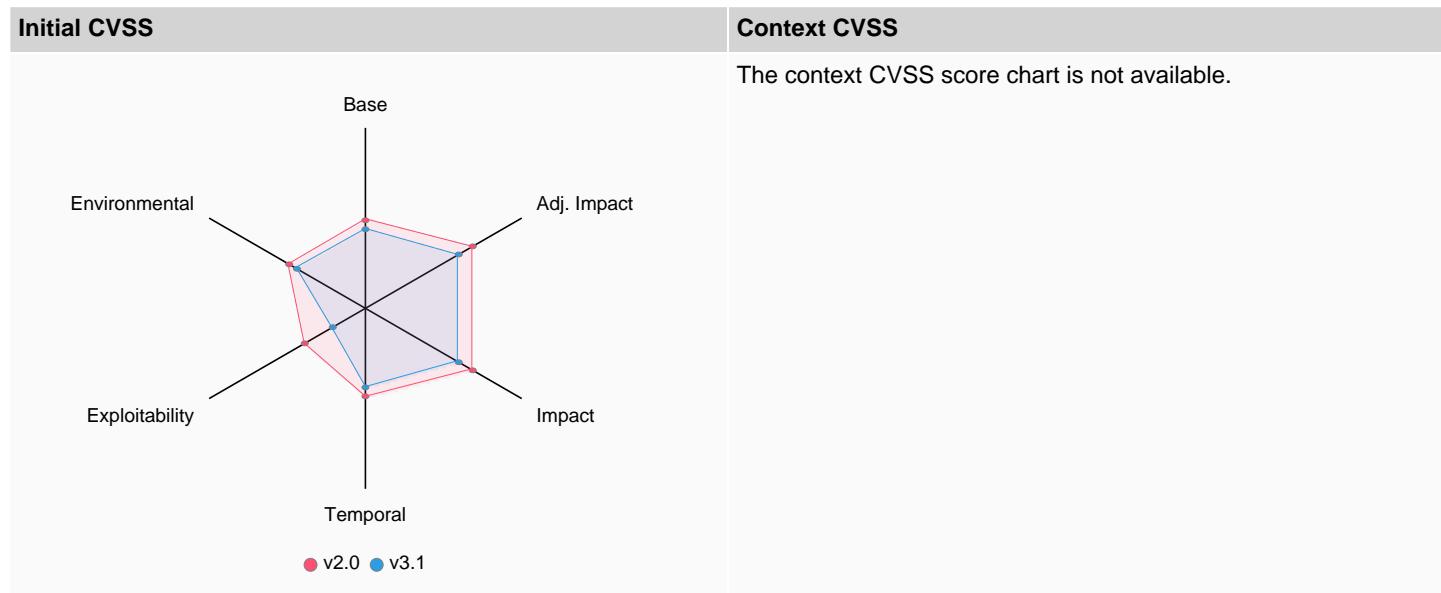


Table 182: CVE-2016-7091 Severity Charts

Rationale

Score is below 7,0

Priority

Elevated (6.4 from base score 4.4)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
Keywords	information disclosure: Confidential or restricted information may be exposed to an adversary. The adversary gains unauthorized access.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2016-2781

Description

chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2016-2781

Table 183: CVE-2016-2781 References

Affected Components

Component	Artifact Id	Version
coreutils-single	coreutils-single-8.32	8.32

Table 184: CVE-2016-2781 Affected Components

Weakness

CWE-20

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.5	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	2.1	AV:L/AC:L/Au:N/C:N/I:P/A:N	Low

Table 185: CVE-2016-2781 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD	6.5	4.0	2.0
CVSS:2.0	NVD-CNA-NVD	2.1	2.9	3.9

Table 186: CVE-2016-2781 Initial Severity Details

Advisories

Alerts

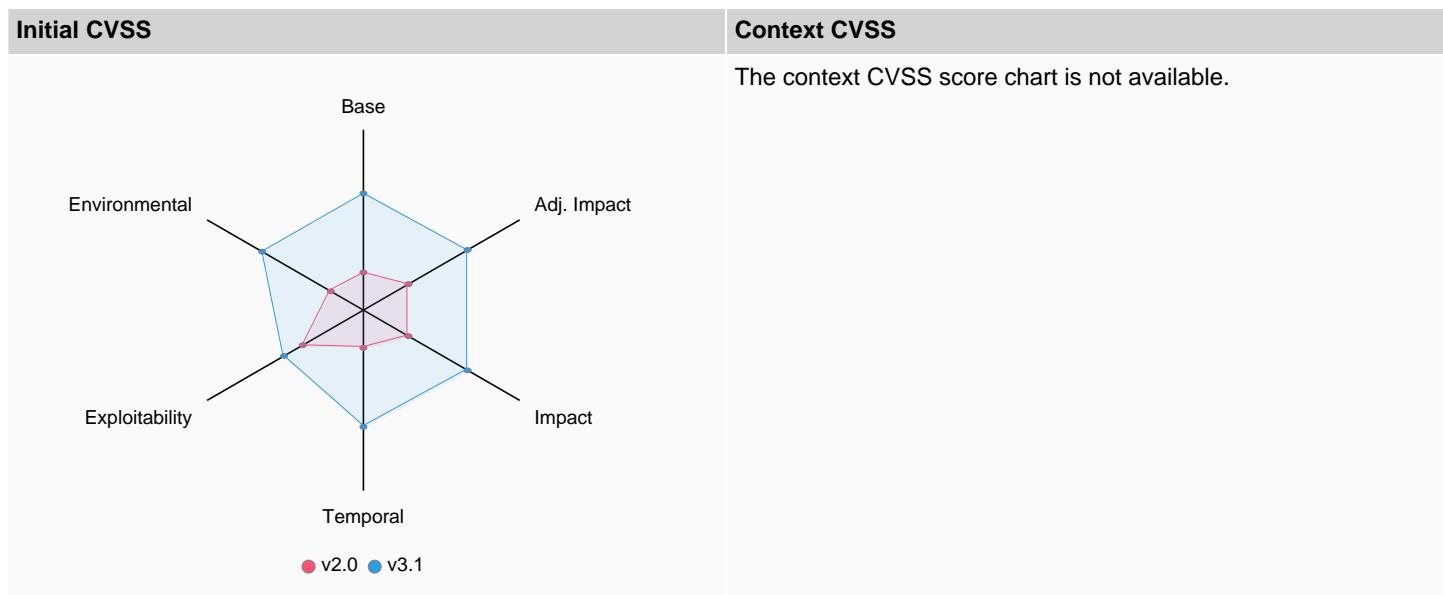
Id	Summary	Create Date	Update Date
GHSA-vf3q-65gx-324p	chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	2022-05-13	2022-05-13

Table 187: CVE-2016-2781 Alerts

Assessment

Summary

Insignificant	Default	Medium
---------------	---------	--------

**Table 188: CVE-2016-2781 Severity Charts****Rationale**

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2013-0136**Description**

Multiple directory traversal vulnerabilities in the EditDocument servlet in the Frontend in Mutiny before 5.0-1.11 allow remote authenticated users to upload and execute arbitrary programs, read arbitrary files, or cause a denial of service (file deletion or renaming) via (1) the uploadPath parameter in an UPLOAD operation; the paths[] parameter in a (2) DELETE, (3) CUT, or (4) COPY operation; or the newPath parameter in a (5) CUT or (6) COPY operation.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2013-0136

Table 189: CVE-2013-0136 References**Affected Components**

Component	Artifact Id	Version
	io.quarkus.quarkus-mutiny-3.8.5.jar	3.8.5

Component	Artifact Id	Version
	io.quarkus.quarkus-mutiny-deployment-3.8.5.jar	3.8.5

Table 190: CVE-2013-0136 Affected Components**Weakness**

CWE-22

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	8.5	AV:N/AC:M/Au:S/C:C/I:C/A:C	High

Table 191: CVE-2013-0136 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:2.0	NVD-CNA-NVD	8.5	10.0	6.8

Table 192: CVE-2013-0136 Initial Severity Details**Advisories****Alerts**

Id		Summary	Create Date	Update Date
VU#701572		Mutiny Appliance contains multiple directory traversal vulnerabilities	2013-04-02	2013-04-02
GHSA-fm6j-565p-53h6		Multiple directory traversal vulnerabilities in the EditDocument servlet in the Frontend in Mutiny before 5.0-1.11 allow remote authenticated users to upload and execute arbitrary programs, read arbitrary files, or cause a denial of service (file deletion or renaming) via (1) the uploadPath parameter in an UPLOAD operation; the paths[] parameter in a (2) DELETE, (3) CUT, or (4) COPY operation; or the newPath parameter in a (5) CUT or (6) COPY operation.	2022-05-05	2022-05-05

Table 193: CVE-2013-0136 Alerts**Assessment****Summary**

In Review

Escalate

High

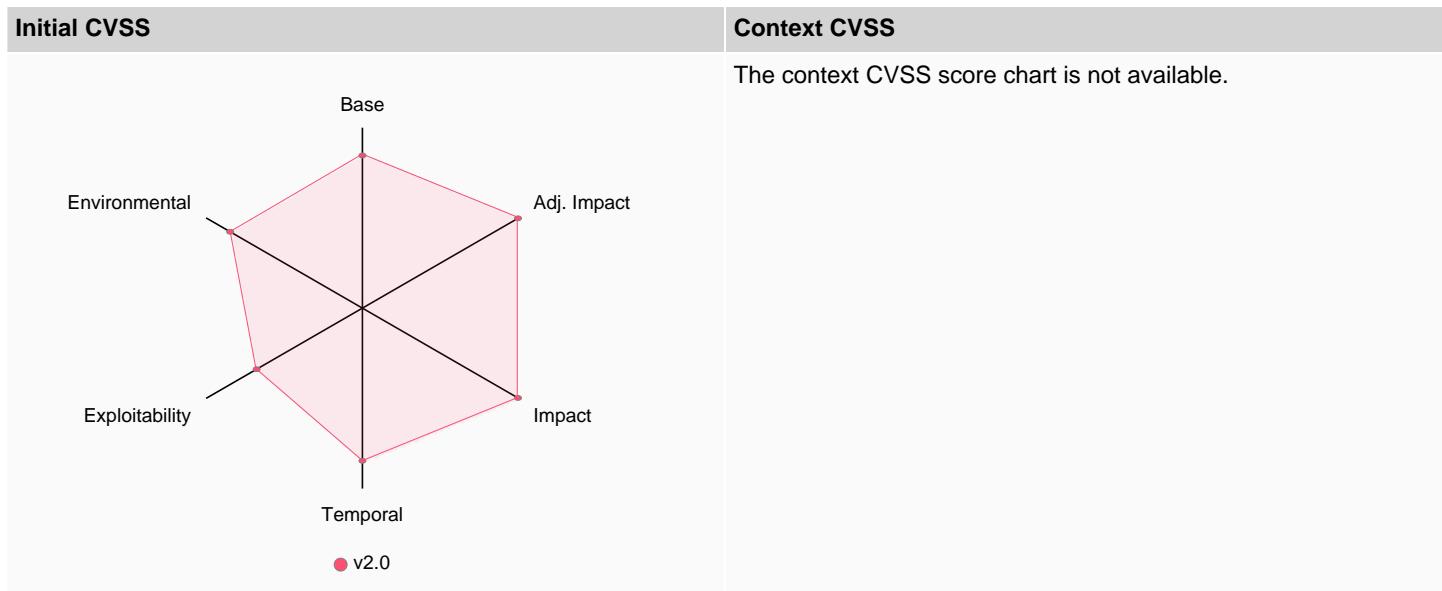


Table 194: CVE-2013-0136 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (9.5 from base score 8.5)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: <code>AV:N/AC:M/Au:S/C:C/I:C/A:C</code>
Keywords	resource exemption: An adversary may attempt to exhaust resources of the system compromising performance objectives and availability.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2011-0536

Description

Multiple untrusted search path vulnerabilities in elf/dl-object.c in certain modified versions of the GNU C Library (aka glibc or libc6), including glibc-2.5-49.el5_5.6 and glibc-2.12-1.7.el6_0.3 in Red Hat Enterprise Linux, allow local users to gain privileges via a crafted dynamic shared object (DSO) in a subdirectory of the current working directory during execution of a (1) setuid or (2) setgid program that has \$ORIGIN in (a) RPATH or (b) RUNPATH within the program itself or a referenced library. NOTE: this issue exists because of an incorrect fix for CVE-2010-3847.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2011-0536

Table 195: CVE-2011-0536 References

Affected Components

Component	Artifact Id	Version
redhat-release	redhat-release-9.4	9.4

Table 196: CVE-2011-0536 Affected Components**Initial Severity**

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.9	AV:L/AC:M/Au:N/C:C/I:C/A:C	Medium

Table 197: CVE-2011-0536 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:2.0	NVD-CNA-NVD	6.9	10.0	3.4

Table 198: CVE-2011-0536 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-3hm4-67xr-p92g	Multiple untrusted search path vulnerabilities in elf/dl-object.c in certain modified versions of the GNU C Library (aka glibc or libc6), including glibc-2.5-49.el5_5.6 and glibc-2.12-1.7.el6_0.3 in Red Hat Enterprise Linux, allow local users to gain privileges via a crafted dynamic shared object (DSO) in a subdirectory of the current working directory during execution of a (1) setuid or (2) setgid program that has \$ORIGIN in (a) RPATH or (b) RUNPATH within the program itself or a referenced library. NOTE: this issue exists because of an incorrect fix for CVE-2010-3847.	2022-05-14	2022-05-14

Table 199: CVE-2011-0536 Alerts**Assessment****Summary**

Insignificant	Default	Medium
---------------	---------	--------

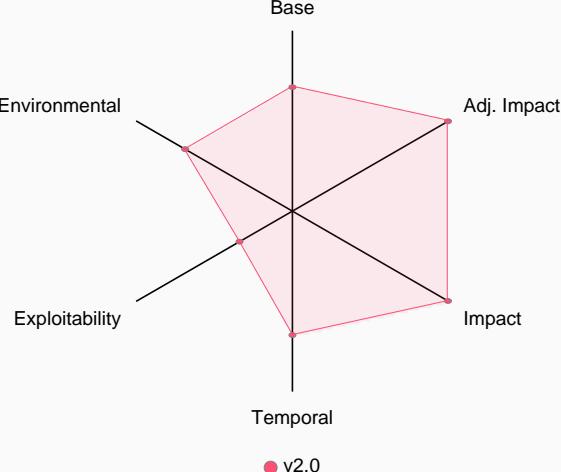
Initial CVSS	Context CVSS
 <p>v2.0</p>	The context CVSS score chart is not available.

Table 200: CVE-2011-0536 Severity Charts**Rationale**

Score is below 7,0

Priority

Default	No elevated priority.
----------------	-----------------------

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:M/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

CVE-2010-4756**Description**

The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2010-4756

Table 201: CVE-2010-4756 References**Affected Components**

Component	Artifact Id	Version
glibc	glibc-2.34	2.34
glibc-common	glibc-common-2.34	2.34

Component	Artifact Id	Version
glibc-langpack-en	glibc-langpack-en-2.34	2.34

Table 202: CVE-2010-4756 Affected Components**Weakness**

CWE-399

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.0	AV:N/AC:L/Au:S/C:N/I:N/A:P	Medium

Table 203: CVE-2010-4756 Initial Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:2.0	NVD-CNA-NVD	4.0	2.9	8.0

Table 204: CVE-2010-4756 Initial Severity Details**Advisories****Alerts**

Id	Summary	Create Date	Update Date
GHSA-x2r9-jfp-jvp9	The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.	2022-05-13	2022-05-13

Table 205: CVE-2010-4756 Alerts**Assessment****Summary**

Insignificant	Elevated	Medium
---------------	----------	--------

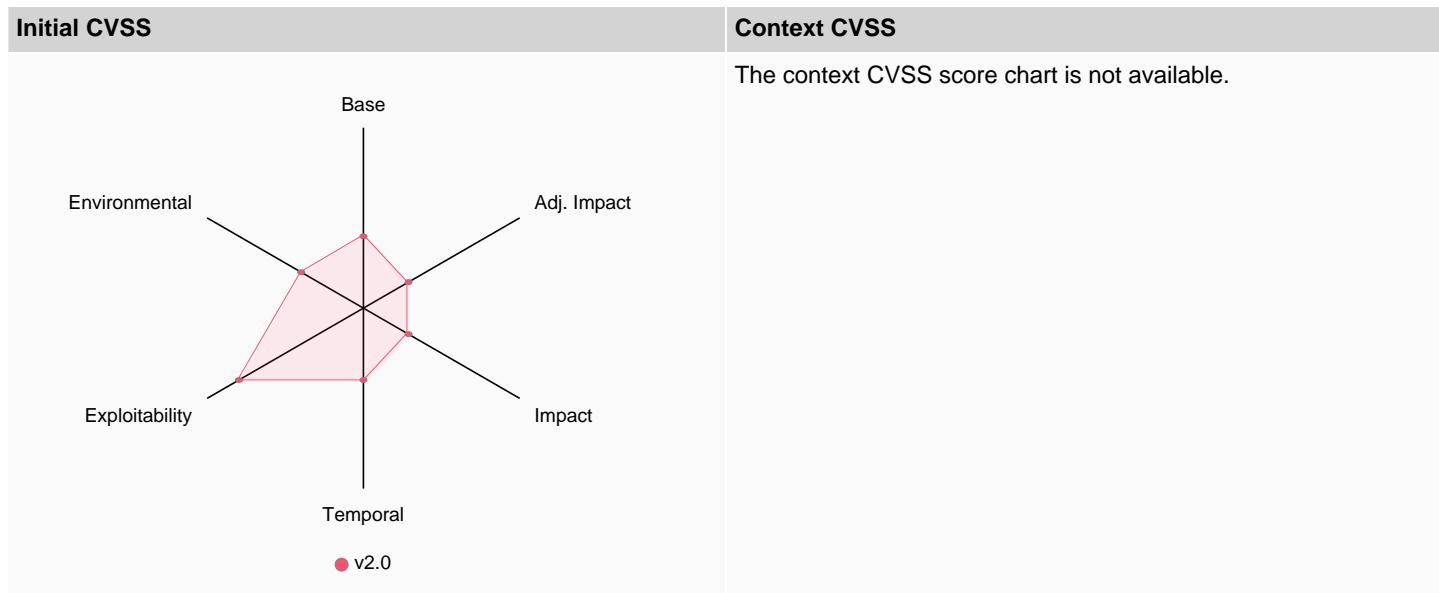


Table 206: CVE-2010-4756 Severity Charts

Rationale

Score is below 7,0

Priority

Elevated (5.0 from base score 4.0)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:S/C:N/I:N/A:P
Keywords	resource exemption: An adversary may attempt to exhaust resources of the system compromising performance objectives and availability.
EPSS	No EPSS score available.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No EOL information available.

List of Tables

Table 1: CVSS Severity Scheme.....	4
Table 2: Overview Charts.....	7
Table 3: Vulnerability Statistics.....	8
Table 4: Vulnerability Statistics with CERT-EU Advisories.....	8
Table 5: Context Vulnerability Statistics.....	8
Table 6: Context Vulnerability Statistics with CERT-EU Advisories.....	9
Table 7: CISA KEV vulnerabilities statistics.....	9
Table 8: In Review Category.....	10
Table 9: Insignificant Category.....	12
Table 10: CVE-2023-7104 References.....	14
Table 11: CVE-2023-7104 Affected Components.....	14
Table 12: CVE-2023-7104 Initial Severity.....	14
Table 13: CVE-2023-7104 Initial Severity Details.....	14
Table 14: CVE-2023-7104 Alerts.....	15
Table 15: CVE-2023-7104 Severity Charts.....	15
Table 16: CVE-2023-6841 References.....	16
Table 17: CVE-2023-6841 Affected Components.....	16
Table 18: CVE-2023-6841 Initial Severity.....	16
Table 19: CVE-2023-6841 Initial Severity Details.....	16
Table 20: CVE-2023-6841 Alerts.....	16
Table 21: CVE-2023-6841 Severity Charts.....	17
Table 22: CVE-2023-5156 References.....	17
Table 23: CVE-2023-5156 Affected Components.....	18
Table 24: CVE-2023-5156 Initial Severity.....	18
Table 25: CVE-2023-5156 Initial Severity Details.....	18
Table 26: CVE-2023-5156 Alerts.....	18
Table 27: CVE-2023-5156 Severity Charts.....	19
Table 28: CVE-2023-4911 References.....	19
Table 29: CVE-2023-4911 Affected Components.....	19
Table 30: CVE-2023-4911 Initial Severity.....	20

Table 31: CVE-2023-4911 Initial Severity Details.....	20
Table 32: CVE-2023-4911 Alerts.....	20
Table 33: CVE-2023-4911 Severity Charts.....	21
Table 34: CVE-2023-4813 References.....	22
Table 35: CVE-2023-4813 Affected Components.....	22
Table 36: CVE-2023-4813 Initial Severity.....	22
Table 37: CVE-2023-4813 Initial Severity Details.....	22
Table 38: CVE-2023-4813 Alerts.....	22
Table 39: CVE-2023-4813 Severity Charts.....	23
Table 40: CVE-2023-45853 References.....	23
Table 41: CVE-2023-45853 Affected Components.....	24
Table 42: CVE-2023-45853 Initial Severity.....	24
Table 43: CVE-2023-45853 Initial Severity Details.....	24
Table 44: CVE-2023-45853 Alerts.....	24
Table 45: CVE-2023-45853 Severity Charts.....	25
Table 46: CVE-2023-4527 References.....	25
Table 47: CVE-2023-4527 Affected Components.....	25
Table 48: CVE-2023-4527 Initial Severity.....	26
Table 49: CVE-2023-4527 Initial Severity Details.....	26
Table 50: CVE-2023-4527 Alerts.....	26
Table 51: CVE-2023-4527 Severity Charts.....	27
Table 52: CVE-2023-4039 References.....	27
Table 53: CVE-2023-4039 Affected Components.....	28
Table 54: CVE-2023-4039 Initial Severity.....	28
Table 55: CVE-2023-4039 Initial Severity Details.....	28
Table 56: CVE-2023-4039 Severity Charts.....	28
Table 57: CVE-2023-29491 References.....	29
Table 58: CVE-2023-29491 Affected Components.....	29
Table 59: CVE-2023-29491 Initial Severity.....	29
Table 60: CVE-2023-29491 Initial Severity Details.....	29
Table 61: CVE-2023-29491 Alerts.....	30
Table 62: CVE-2023-29491 Severity Charts.....	30

Table 63: CVE-2023-2603 References.....	31
Table 64: CVE-2023-2603 Affected Components.....	31
Table 65: CVE-2023-2603 Initial Severity.....	31
Table 66: CVE-2023-2603 Initial Severity Details.....	31
Table 67: CVE-2023-2603 Alerts.....	31
Table 68: CVE-2023-2603 Severity Charts.....	32
Table 69: CVE-2023-0687 References.....	32
Table 70: CVE-2023-0687 Affected Components.....	33
Table 71: CVE-2023-0687 Initial Severity.....	33
Table 72: CVE-2023-0687 Initial Severity Details.....	33
Table 73: CVE-2023-0687 Alerts.....	33
Table 74: CVE-2023-0687 Severity Charts.....	34
Table 75: CVE-2022-41409 References.....	34
Table 76: CVE-2022-41409 Affected Components.....	34
Table 77: CVE-2022-41409 Initial Severity.....	35
Table 78: CVE-2022-41409 Initial Severity Details.....	35
Table 79: CVE-2022-41409 Alerts.....	35
Table 80: CVE-2022-41409 Severity Charts.....	36
Table 81: CVE-2022-37832 References.....	36
Table 82: CVE-2022-37832 Affected Components.....	36
Table 83: CVE-2022-37832 Initial Severity.....	37
Table 84: CVE-2022-37832 Initial Severity Details.....	37
Table 85: CVE-2022-37832 Alerts.....	37
Table 86: CVE-2022-37832 Severity Charts.....	37
Table 87: CVE-2022-37434 References.....	38
Table 88: CVE-2022-37434 Affected Components.....	38
Table 89: CVE-2022-37434 Initial Severity.....	38
Table 90: CVE-2022-37434 Initial Severity Details.....	38
Table 91: CVE-2022-37434 Alerts.....	39
Table 92: CVE-2022-37434 Severity Charts.....	39
Table 93: CVE-2022-35737 References.....	40
Table 94: CVE-2022-35737 Affected Components.....	40

Table 95: CVE-2022-35737 Initial Severity.....	40
Table 96: CVE-2022-35737 Initial Severity Details.....	40
Table 97: CVE-2022-35737 Alerts.....	40
Table 98: CVE-2022-35737 Severity Charts.....	41
Table 99: CVE-2022-29458 References.....	41
Table 100: CVE-2022-29458 Affected Components.....	41
Table 101: CVE-2022-29458 Initial Severity.....	42
Table 102: CVE-2022-29458 Initial Severity Details.....	42
Table 103: CVE-2022-29458 Alerts.....	42
Table 104: CVE-2022-29458 Severity Charts.....	43
Table 105: CVE-2022-23219 References.....	43
Table 106: CVE-2022-23219 Affected Components.....	43
Table 107: CVE-2022-23219 Initial Severity.....	44
Table 108: CVE-2022-23219 Initial Severity Details.....	44
Table 109: CVE-2022-23219 Alerts.....	44
Table 110: CVE-2022-23219 Severity Charts.....	45
Table 111: CVE-2022-23218 References.....	45
Table 112: CVE-2022-23218 Affected Components.....	45
Table 113: CVE-2022-23218 Initial Severity.....	46
Table 114: CVE-2022-23218 Initial Severity Details.....	46
Table 115: CVE-2022-23218 Alerts.....	46
Table 116: CVE-2022-23218 Severity Charts.....	47
Table 117: CVE-2021-46848 References.....	47
Table 118: CVE-2021-46848 Affected Components.....	47
Table 119: CVE-2021-46848 Initial Severity.....	48
Table 120: CVE-2021-46848 Initial Severity Details.....	48
Table 121: CVE-2021-46848 Alerts.....	48
Table 122: CVE-2021-46848 Severity Charts.....	48
Table 123: CVE-2021-43396 References.....	49
Table 124: CVE-2021-43396 Affected Components.....	49
Table 125: CVE-2021-43396 Initial Severity.....	49
Table 126: CVE-2021-43396 Initial Severity Details.....	49

Table 127: CVE-2021-43396 Alerts.....	50
Table 128: CVE-2021-43396 Severity Charts.....	50
Table 129: CVE-2021-3998 References.....	51
Table 130: CVE-2021-3998 Affected Components.....	51
Table 131: CVE-2021-3998 Initial Severity.....	51
Table 132: CVE-2021-3998 Initial Severity Details.....	51
Table 133: CVE-2021-3998 Alerts.....	51
Table 134: CVE-2021-3998 Severity Charts.....	52
Table 135: CVE-2021-39537 References.....	52
Table 136: CVE-2021-39537 Affected Components.....	52
Table 137: CVE-2021-39537 Initial Severity.....	53
Table 138: CVE-2021-39537 Initial Severity Details.....	53
Table 139: CVE-2021-39537 Alerts.....	53
Table 140: CVE-2021-39537 Severity Charts.....	53
Table 141: CVE-2021-38604 References.....	54
Table 142: CVE-2021-38604 Affected Components.....	54
Table 143: CVE-2021-38604 Initial Severity.....	54
Table 144: CVE-2021-38604 Initial Severity Details.....	54
Table 145: CVE-2021-38604 Alerts.....	55
Table 146: CVE-2021-38604 Severity Charts.....	55
Table 147: CVE-2020-25638 References.....	56
Table 148: CVE-2020-25638 Affected Components.....	56
Table 149: CVE-2020-25638 Initial Severity.....	56
Table 150: CVE-2020-25638 Initial Severity Details.....	56
Table 151: CVE-2020-25638 Alerts.....	57
Table 152: CVE-2020-25638 Severity Charts.....	57
Table 153: CVE-2020-13956 References.....	58
Table 154: CVE-2020-13956 Affected Components.....	58
Table 155: CVE-2020-13956 Initial Severity.....	58
Table 156: CVE-2020-13956 Initial Severity Details.....	58
Table 157: CVE-2020-13956 Alerts.....	58
Table 158: CVE-2020-13956 Severity Charts.....	59

Table 159: CVE-2019-14900 References.....	59
Table 160: CVE-2019-14900 Affected Components.....	59
Table 161: CVE-2019-14900 Initial Severity.....	60
Table 162: CVE-2019-14900 Initial Severity Details.....	60
Table 163: CVE-2019-14900 Alerts.....	60
Table 164: CVE-2019-14900 Severity Charts.....	61
Table 165: CVE-2018-25032 References.....	61
Table 166: CVE-2018-25032 Affected Components.....	61
Table 167: CVE-2018-25032 Initial Severity.....	62
Table 168: CVE-2018-25032 Initial Severity Details.....	62
Table 169: CVE-2018-25032 Alerts.....	62
Table 170: CVE-2018-25032 Severity Charts.....	62
Table 171: CVE-2018-15529 References.....	63
Table 172: CVE-2018-15529 Affected Components.....	63
Table 173: CVE-2018-15529 Initial Severity.....	63
Table 174: CVE-2018-15529 Initial Severity Details.....	63
Table 175: CVE-2018-15529 Alerts.....	64
Table 176: CVE-2018-15529 Severity Charts.....	64
Table 177: CVE-2016-7091 References.....	65
Table 178: CVE-2016-7091 Affected Components.....	65
Table 179: CVE-2016-7091 Initial Severity.....	65
Table 180: CVE-2016-7091 Initial Severity Details.....	65
Table 181: CVE-2016-7091 Alerts.....	66
Table 182: CVE-2016-7091 Severity Charts.....	66
Table 183: CVE-2016-2781 References.....	67
Table 184: CVE-2016-2781 Affected Components.....	67
Table 185: CVE-2016-2781 Initial Severity.....	67
Table 186: CVE-2016-2781 Initial Severity Details.....	67
Table 187: CVE-2016-2781 Alerts.....	67
Table 188: CVE-2016-2781 Severity Charts.....	68
Table 189: CVE-2013-0136 References.....	68
Table 190: CVE-2013-0136 Affected Components.....	68

Table 191: CVE-2013-0136 Initial Severity.....	69
Table 192: CVE-2013-0136 Initial Severity Details.....	69
Table 193: CVE-2013-0136 Alerts.....	69
Table 194: CVE-2013-0136 Severity Charts.....	70
Table 195: CVE-2011-0536 References.....	70
Table 196: CVE-2011-0536 Affected Components.....	71
Table 197: CVE-2011-0536 Initial Severity.....	71
Table 198: CVE-2011-0536 Initial Severity Details.....	71
Table 199: CVE-2011-0536 Alerts.....	71
Table 200: CVE-2011-0536 Severity Charts.....	72
Table 201: CVE-2010-4756 References.....	72
Table 202: CVE-2010-4756 Affected Components.....	72
Table 203: CVE-2010-4756 Initial Severity.....	73
Table 204: CVE-2010-4756 Initial Severity Details.....	73
Table 205: CVE-2010-4756 Alerts.....	73
Table 206: CVE-2010-4756 Severity Charts.....	74

Glossary

Common Product Enumeration

Common Product Enumeration (CPE) is a scheme used by the [NVD](#) to identify vulnerable products (software and hardware). A CPE has a defined structure consisting of several parts:

```
cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:  
<language>:<sw_edition>:<target_sw>:  
<target_hw>:<other>
```

With a CPE several vulnerabilities ([CVE](#)) can be associated.

Common Vulnerability Exposure

A Common Vulnerability Exposure (CVE) is a public representation of a vulnerability. Each CVE covers a description and machine-readable information for version matching.

Common Vulnerability Scoring System

The severity of vulnerabilities is commonly measured applying the Common Vulnerability Scoring System (CVSS) scoring system. The scheme uses several individual metrics to capture different aspects of a vulnerability.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is a science laboratory and agency of the United States Department of Commerce. Apart from many other activities the NIST publishes the Cybersecurity Framework guidance on information security and risk management.

National Vulnerability Database

The National Vulnerability Database (NVD) is a repository of vulnerability related data. The NVD hosts [CPE](#) and [CVE](#) details for retrieving and matching vulnerability information.

The NVD is managed by the [National Institute of Standards and Technology \(NIST\)](#).