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

metaeffekt GmbH

https://metaeffekt.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

metaeffekt GmbH

https://metaeffekt.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'. metaeffekt GmbH does not claim any copyright on the included external materials nor is metaeffekt GmbH liable for the correctness and completeness of the presented external materials. Materials from external sources are included herein for informational purposes only. metaeffekt 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 metaeffekt GmbH. The fact that such a component has a known vulnerability must not necessarily mean that this vulnerability immediately affects the metaeffekt 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 metaeffekt 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

Contents

1 Vulnerability Overview

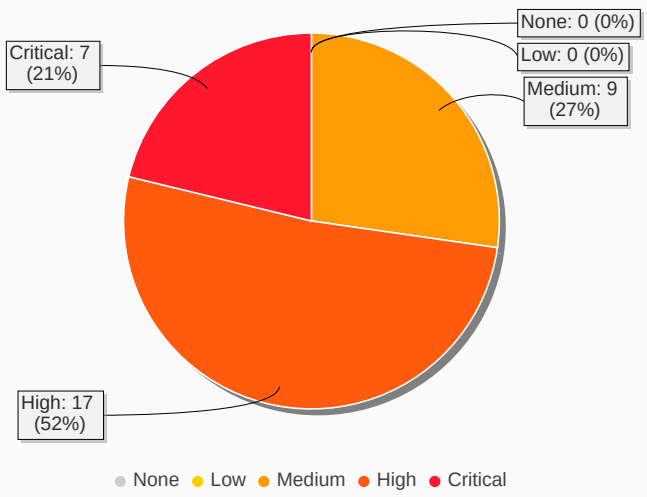
For the third-party components contained in Example vulnerabilities have been queried from public vulnerability databases. The following sections cover the vulnerabilities for the software parts included in Example.

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.

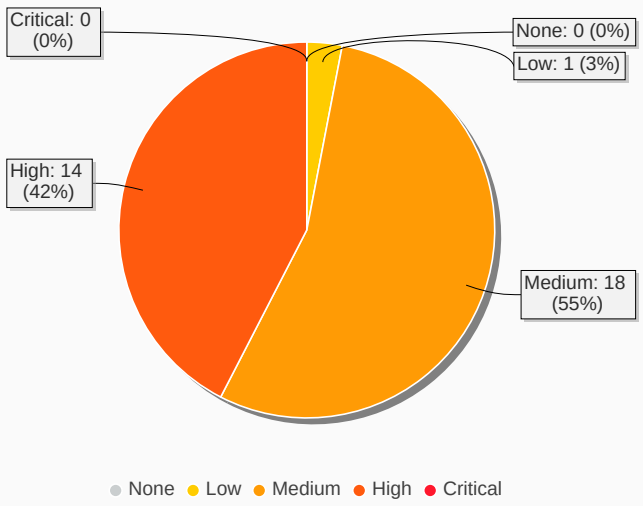
Initial Vulnerability Severity

The chart depicts the vulnerability severity distribution without context information.



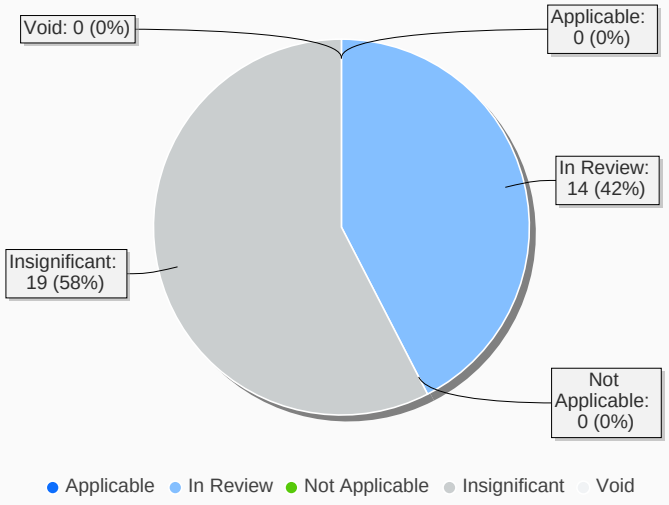
Context Vulnerability Severity

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.

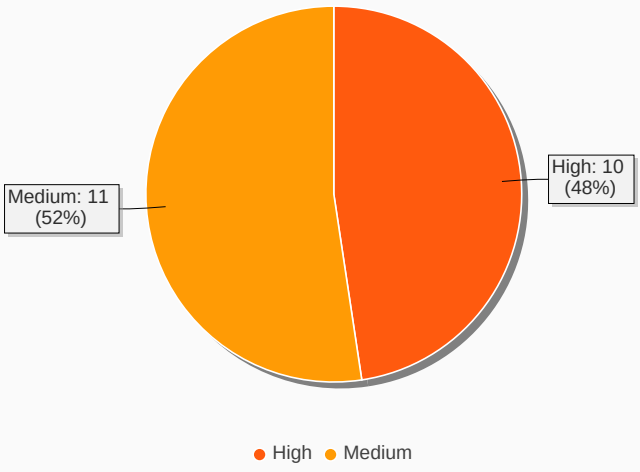


Table 2: Overview Charts

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	0	0	0	0	0	n/a
High	0	14	0	0	0	14	0,0 %
Medium	0	0	0	18	0	18	0,0 %
Low	0	0	0	1	0	1	0,0 %

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	8.8	Critical	High	Default	In Review
	GHSA-mq29-j5xf-cjwr					
	cpe:/a:zlib:zlib [, 1.3]					
CVE-2023-0687	9.8	8.8	Critical	High	Default	In Review
	GHSA-5r4p-4pqv-gqhw					
	cpe:/a:gnu:glibc [, 2.38)					
CVE-2022-37832	9.8	8.8	Critical	High	Default	In Review
	GHSA-999r-r2f8-xm55					
	cpe:/a:mutiny:mutiny [, 7.2.0-10855)					
CVE-2022-37434	9.8	8.8	Critical	High	Default	In Review
	GHSA-cfmr-vrgj-vqwv					
	cpe:/a:zlib:zlib [, 1.2.12]					
CVE-2022-23219	9.8	8.8	Critical	High	Escalate	In Review
	GHSA-fhxm-4mc9-6jf5					
	cpe:/a:gnu:glibc [, 2.34]					
CVE-2022-23218	9.8	8.8	Critical	High	Escalate	In Review
	GHSA-8g8v-256r-57v7					
	cpe:/a:gnu:glibc [, 2.34]					
CVE-2021-46848	9.1	8.1	Critical	High	Default	In Review
	GHSA-6468-68pw-9chw					
	cpe:/a:gnu:libtasn1 [, 4.19.0)					
CVE-2021-39537	8.8	8.0	High	High	Default	In Review

Name	Score	$Score_{ctx}$	Severity	$Severity_{ctx}$	Priority	Status
	GHSA-v5gv-3mwr-6223					
	cpe:/a:gnu:ncurses [, 6.2.1]					
CVE-2018-15529	8.8	8.0	High	High	Default	In Review
	GHSA-9xfc-48gq-9whq					
	cpe:/a:mutiny:mutiny [, 6.1.0-5263)					
CVE-2023-4911	7.8	7.8	High	High	Escalate	In Review
	CERT-EU-2023-072 GHSA-m77w-6vjw-wh2f					
	cpe:/a:gnu:glibc [2.34, 2.39)					
CVE-2023-29491	7.8	7.8	High	High	Default	In Review
	GHSA-vh2x-5rx6-qqhv					
	cpe:/a:gnu:ncurses [, 6.4)					
CVE-2023-2603	7.8	7.8	High	High	Default	In Review
	GHSA-wp54-pwvg-rqq5					
	cpe:/a:libcap_project:libcap [, 2.66-4)					
CVE-2013-0136	8.5	7.4	High	High	Due	In Review
	VU#701572 GHSA-fm6j-565p-53h6					
	cpe:/a:mutiny:mutiny [, 5.0-1.10]					
CVE-2022-29458	7.1	7.1	High	High	Default	In Review
	GHSA-jh4f-5j2m-4v9c					
	cpe:/a:gnu:ncurses [, 6.3)					

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-2023-6841	7.1	6.9	High	Medium	Due	Insignificant
	GHSA-w97f-w3hq-36g2					

Name	Score	$Score_{ctx}$	Severity	$Severity_{ctx}$	Priority	Status
	GHSA org.keycloak:keycloak-core (Maven) [0, 25.0.5]					
CVE-2011-0536	6.9	6.9	Medium	Medium	Default	Insignificant
	GHSA-3hm4-67xr-p92g					
	cpe:/o:redhat:enterprise_linux					
CVE-2020-25638	7.4	6.8	High	Medium	Escalate	Insignificant
	GHSA-j8jw-g6fq-mp7h					
	cpe:/a:hibernate:hibernate_orm [, 5.3.20)					
CVE-2023-5156	7.5	6.5	High	Medium	Due	Insignificant
	GHSA-m7p3-g2hx-xfc3					
	cpe:/a:gnu:glibc [2.34, 2.39)					
CVE-2022-41409	7.5	6.5	High	Medium	Due	Insignificant
	GHSA-4qfx-v7wh-3q4j					
	cpe:/a:pcre:pcre2 [, 10.41)					
CVE-2022-35737	7.5	6.5	High	Medium	Default	Insignificant
	GHSA-jw36-hf63-69r9					
	cpe:/a:sqlite:sqlite [1.0.12, 3.39.2)					
CVE-2021-43396	7.5	6.5	High	Medium	Escalate	Insignificant
	GHSA-73g2-m4v3-6c2h					
	cpe:/a:gnu:glibc:2.34 2.34 (*)					
CVE-2021-3998	7.5	6.5	High	Medium	Default	Insignificant
	GHSA-32pr-wg5j-9rwr					
	cpe:/a:gnu:glibc [2.33, 2.35)					
CVE-2021-38604	7.5	6.5	High	Medium	Default	Insignificant
	GHSA-p3v7-wjmc-7fh8					
	cpe:/a:gnu:glibc [, 2.34]					
CVE-2018-25032	7.5	6.5	High	Medium	Default	Insignificant
	GHSA-jc36-42cf-vqwj					
	cpe:/a:zlib:zlib [, 1.2.12)					
CVE-2016-2781	6.5	6.5	Medium	Medium	Default	Insignificant
	GHSA-vf3q-65gx-324p					
	cpe:/a:gnu:coreutils					

Name	Score	$Score_{ctx}$	Severity	$Severity_{ctx}$	Priority	Status
CVE-2023-7104	7.3	6.3	High	Medium	Default	Insignificant
	GHSA-f92h-rw3f-8j92					
	cpe:/a:sqlite:sqlite [, 3.43.0]					
CVE-2023-4527	6.5	5.9	Medium	Medium	Default	Insignificant
	GHSA-hmf7-f8gf-8f4p					
	cpe:/a:gnu:glibc [, 2.39)					
CVE-2019-14900	6.5	5.7	Medium	Medium	Due	Insignificant
	GHSA-8grg-q944-cch5					
	cpe:/a:hibernate:hibernate_orm [, 5.3.18)					
CVE-2023-4813	5.9	5.3	Medium	Medium	Default	Insignificant
	GHSA-qx6j-g797-jg9r					
	cpe:/a:gnu:glibc [, 2.36)					
CVE-2016-7091	4.4	4.4	Medium	Medium	Elevated	Insignificant
	GHSA-4h4j-rqc9-6rq3					
	cpe:/o:redhat:enterprise_linux					
CVE-2020-13956	5.3	4.3	Medium	Medium	Default	Insignificant
	GHSA-7r82-7xv7-xcpj					
	cpe:/a:apache:httpclient [, 4.5.13)					
CVE-2023-4039	4.8	4.2	Medium	Medium	Default	Insignificant
	cpe:/a:gnu:gcc:::~~~~arm64~ [, 2023-09-12)					
CVE-2010-4756	4.0	2.7	Medium	Low	Elevated	Insignificant
	GHSA-x2r9-jfjp-jvp9					
	cpe:/a:gnu:glibc					

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

Insignificant Default Medium

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	6.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/MAV:A	Medium
CVSS:2.0	NVD-CNA-VulDB + Assessment	5.2	AV:A/AC:L/Au:S/C:P/I:P/A:P	Medium

Table 15: CVE-2023-7104 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.3	3.4	3.9	6.3	3.4
CVSS:2.0	NVD-CNA-VulDB + Assessment	5.2	6.4	5.1		

Table 16: CVE-2023-7104 Context Severity Details

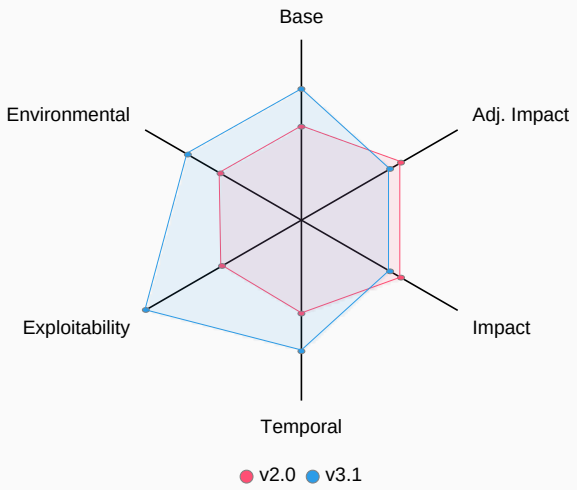
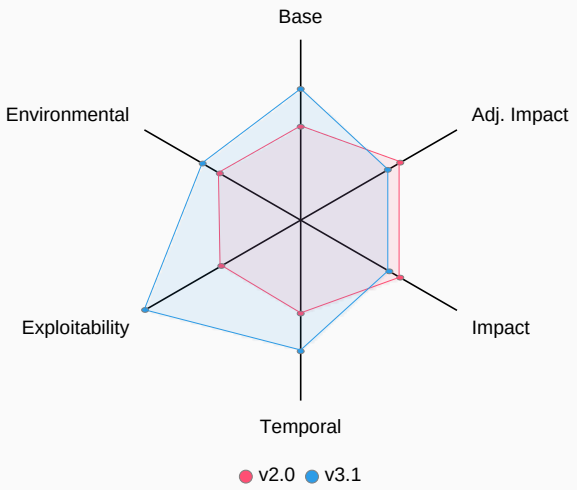
Initial CVSS	Context CVSS
	

Table 17: CVE-2023-7104 Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/MAV:A`
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	sqlite (ver. 3) is still supported by it's 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 18: CVE-2023-6841 References

Affected Components

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

Table 19: 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 20: 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 21: 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 22: CVE-2023-6841 Alerts

Assessment

Summary

Insignificant Due Medium

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:4.0	GitHub, Inc. + Assessment	6.9	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/MAV:A	Medium
CVSS:3.1	GitHub, Inc. + Assessment	5.7	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/MAV:A	Medium

Table 23: CVE-2023-6841 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:4.0	GitHub, Inc. + Assessment	6.9				

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	GitHub, Inc. + Assessment	6.5	3.6	2.8	5.7	3.6

Table 24: CVE-2023-6841 Context Severity Details

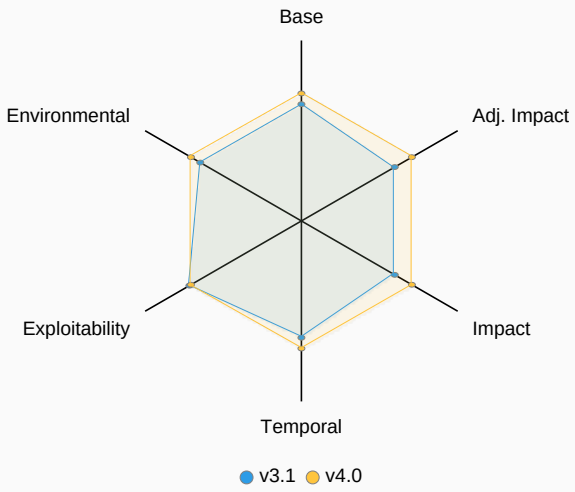
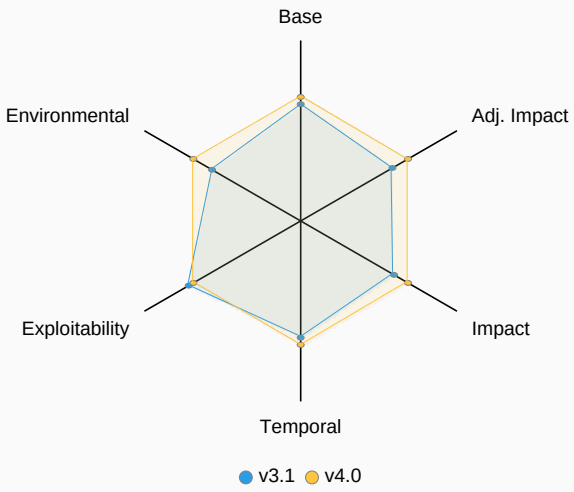
Initial CVSS	Context CVSS
	

Table 25: CVE-2023-6841 Severity Charts

Rationale
Score is below 7,0

Priority

Due (**7.9** from base score **6.9**)

Criteria	Explanation
CVSS Overall	*CVSS:4.0 GitHub, Inc. + Assessment-lower* provides the vector: `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/MAV:A`
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 26: CVE-2023-5156 References

Affected Components

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

Table 27: 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 28: CVE-2023-5156 Initial Severity

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

Table 29: 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 30: CVE-2023-5156 Alerts

Assessment

Summary

Insignificant Due Medium

Context Severity

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

Table 31: CVE-2023-5156 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.5	3.6	3.9	6.5	3.6

Table 32: CVE-2023-5156 Context Severity Details

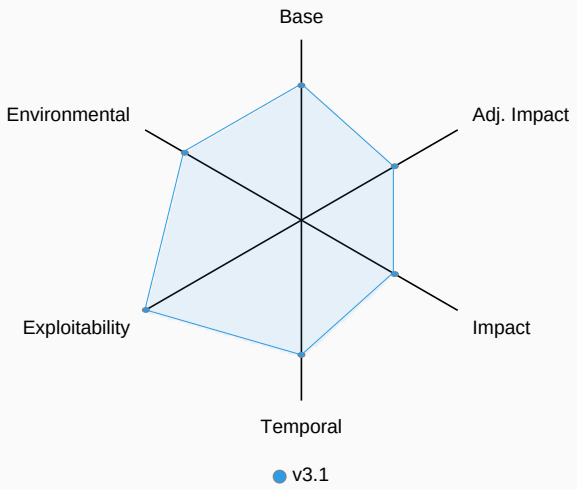
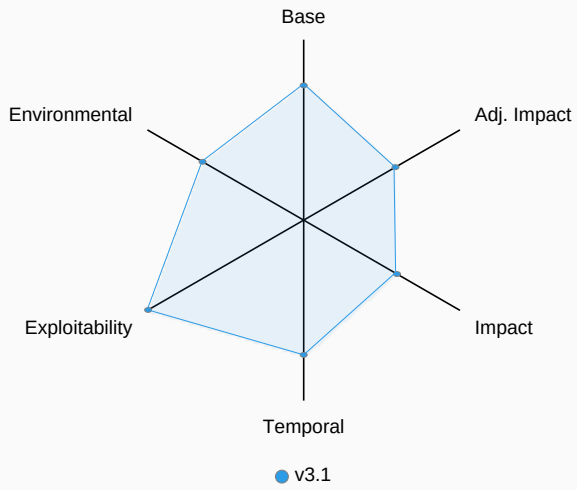
Initial CVSS	Context CVSS
	

Table 33: CVE-2023-5156 Severity Charts

Rationale
Score is below 7,0

Priority

Due (**7.5** from base score **6.5**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A`
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 34: CVE-2023-4911 References

Affected Components

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

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

Table 35: 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 36: CVE-2023-4911 Initial Severity

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

Table 37: CVE-2023-4911 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
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
CERT-EU-2023-072	GNU C Library Dynamic Loader Buffer Overflow Vulnerability	2023-10-04	2023-10-04

Table 38: CVE-2023-4911 Alerts

Assessment

Summary

In Review Escalate High

Context Severity

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

Table 39: CVE-2023-4911 Context Severity

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

Table 40: CVE-2023-4911 Context Severity Details

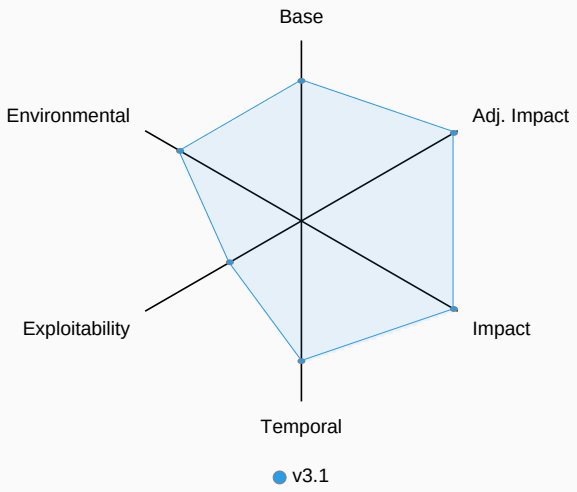
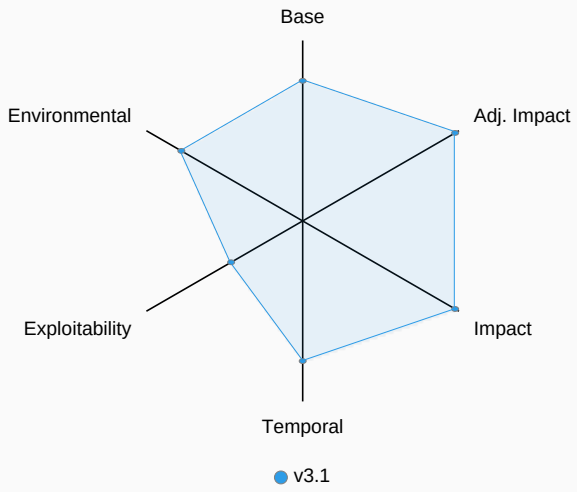
Initial CVSS	Context CVSS
	

Table 41: 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 + Assessment-lower* 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, affecting **GNU 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 42: CVE-2023-4813 References

Affected Components

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

Table 43: 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 44: CVE-2023-4813 Initial Severity

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

Table 45: 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 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.	2023-09-13	2023-09-13

Table 46: CVE-2023-4813 Alerts

Assessment

Summary

Insignificant | Default | **Medium**

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	5.3	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A	Medium

Table 47: CVE-2023-4813 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	5.9	3.6	2.2	5.3	3.6

Table 48: CVE-2023-4813 Context Severity Details

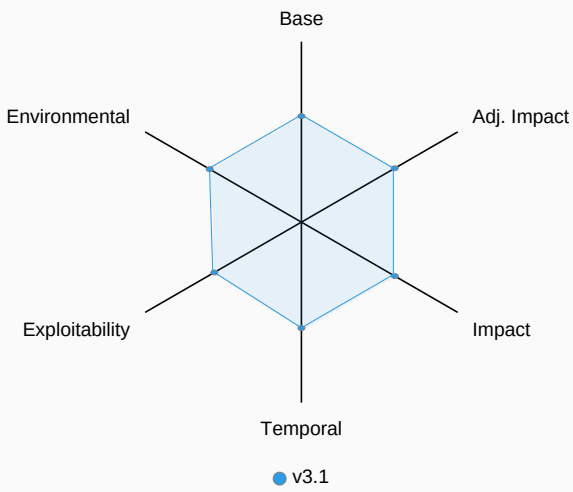
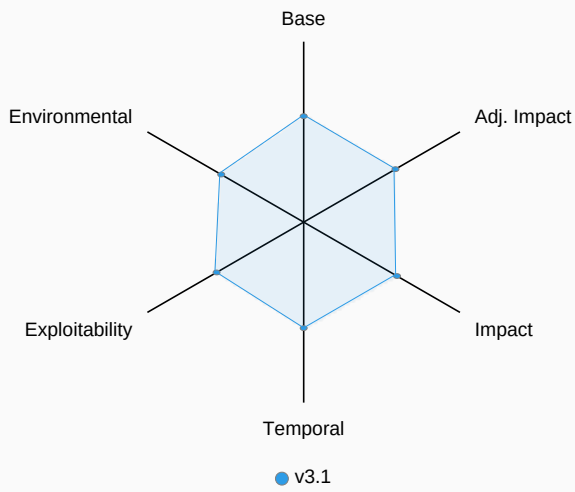
Initial CVSS	Context CVSS
	

Table 49: 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 + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A
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 50: CVE-2023-45853 References

Affected Components

Component	Artifact Id	Version
zlib	`zlib-1.2.11`	`1.2.11`

Table 51: 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 52: CVE-2023-45853 Initial Severity

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

Table 53: 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 54: CVE-2023-45853 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A	High

Table 55: CVE-2023-45853 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	9.8	5.9	3.9	8.8	5.9

Table 56: CVE-2023-45853 Context Severity Details

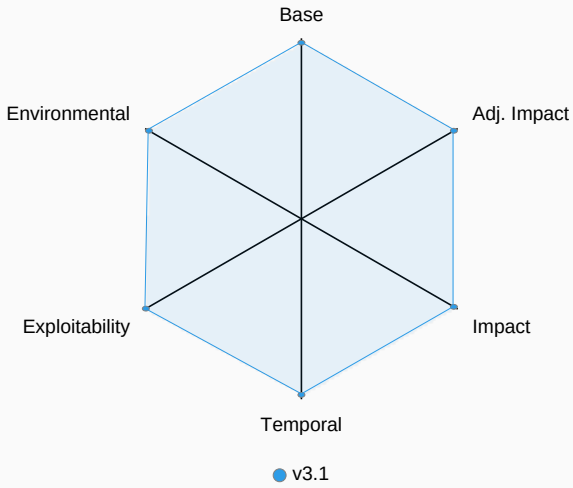
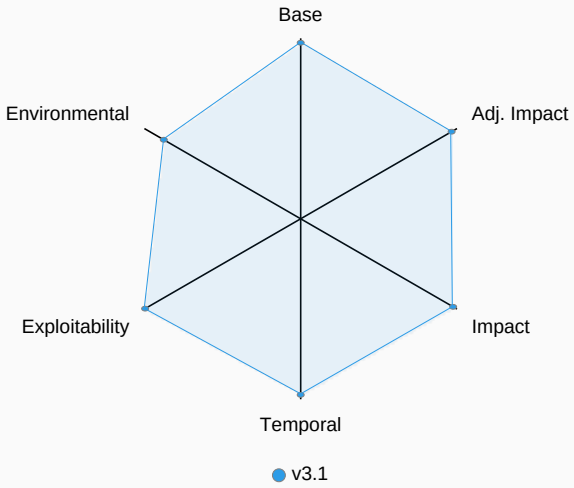
Initial CVSS	Context CVSS
	

Table 57: 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 + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A
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 58: CVE-2023-4527 References

Affected Components

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

Table 59: 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 60: CVE-2023-4527 Initial Severity

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

Table 61: 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 62: CVE-2023-4527 Alerts

Assessment

Summary

Insignificant | Default | **Medium**

Context Severity

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

Table 63: CVE-2023-4527 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	6.5	4.2	2.2	5.9	4.2

Table 64: CVE-2023-4527 Context Severity Details

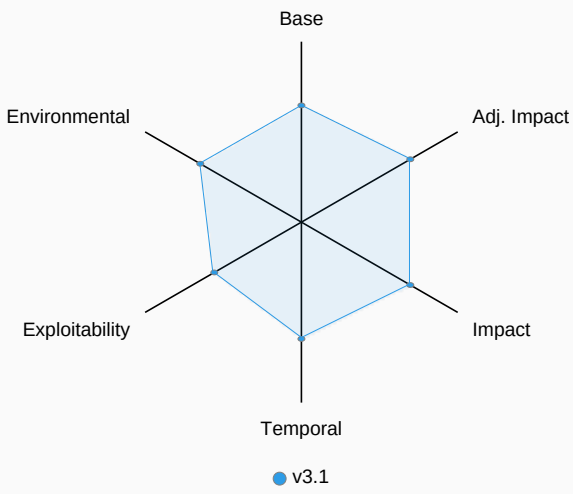
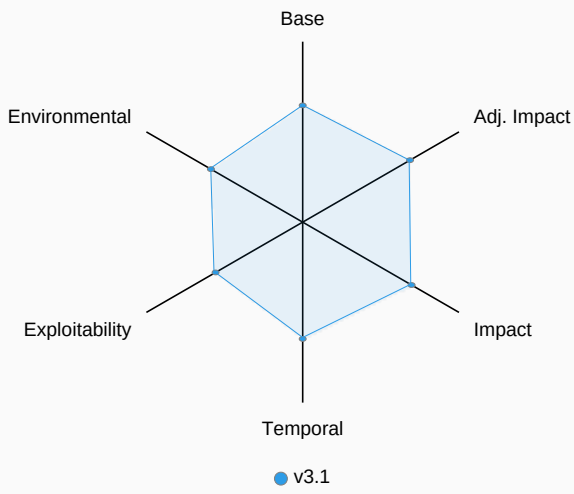
Initial CVSS	Context CVSS
	

Table 65: 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 + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H/MAV:A
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

DISPUTEDA 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 66: CVE-2023-4039 References

Affected Components

Component	Artifact Id	Version
libgcc	`libgcc-11.4.1`	`11.4.1`

Table 67: 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 68: CVE-2023-4039 Initial Severity

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

Table 69: CVE-2023-4039 Initial Severity Details

Advisories

No security advisories have been identified.

Assessment

Summary

Insignificant | Default | **Medium**

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	4.2	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/MAV:A	Medium

Table 70: CVE-2023-4039 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	4.8	2.5	2.2	4.2	2.5

Table 71: CVE-2023-4039 Context Severity Details

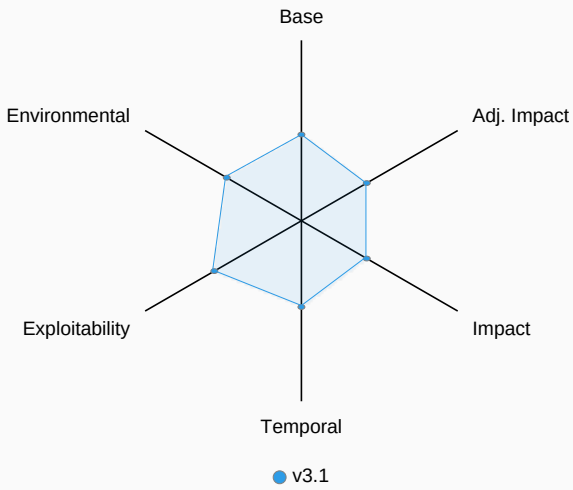
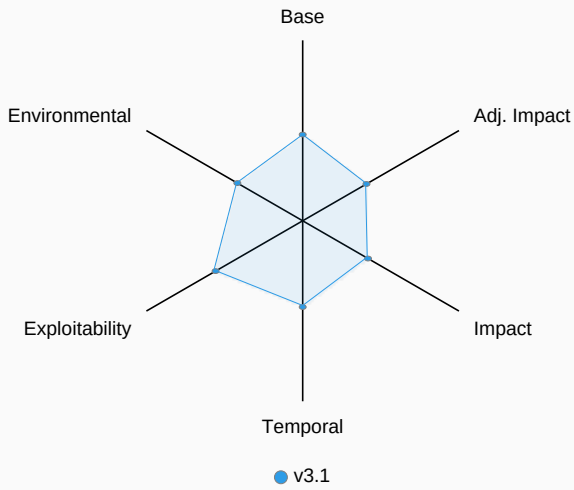
Initial CVSS	Context CVSS
	

Table 72: 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 + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/MAV:A
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 73: 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 74: 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 75: CVE-2023-29491 Initial Severity

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

Table 76: 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 77: CVE-2023-29491 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

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

Table 78: CVE-2023-29491 Context Severity

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

Table 79: CVE-2023-29491 Context Severity Details

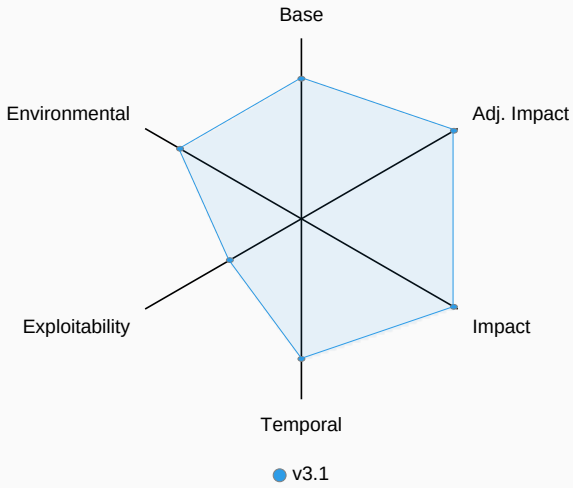
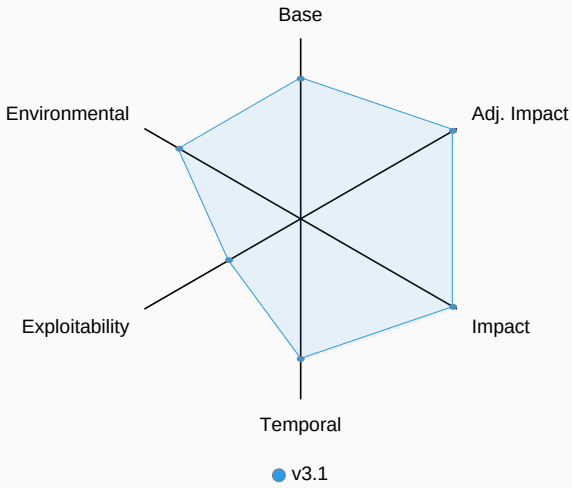
Initial CVSS	Context CVSS
	

Table 80: 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 + Assessment-lower* 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 81: CVE-2023-2603 References

Affected Components

Component	Artifact Id	Version
libcap	`libcap-2.48`	`2.48`

Table 82: 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 83: CVE-2023-2603 Initial Severity

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

Table 84: 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 _libcap_strdup() function and can lead to an integer overflow if the input string is close to 4GiB.	2023-06-06	2023-06-06

Table 85: CVE-2023-2603 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

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

Table 86: CVE-2023-2603 Context Severity

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

Table 87: CVE-2023-2603 Context Severity Details

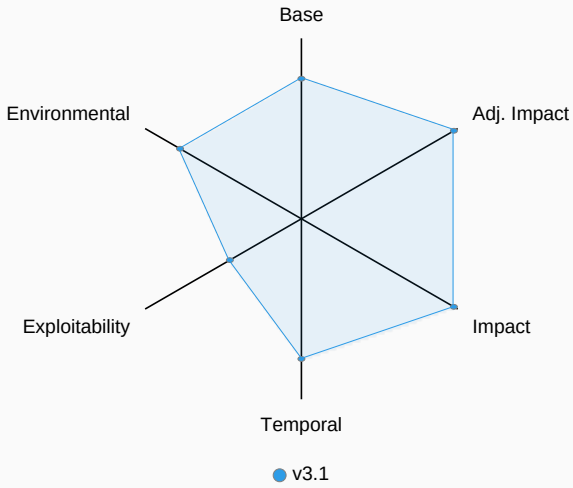
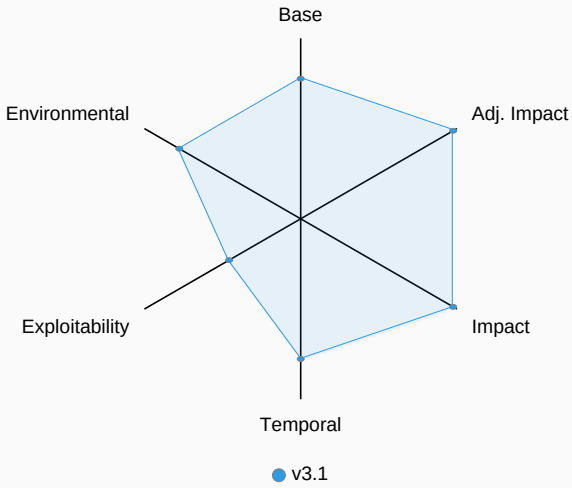
Initial CVSS	Context CVSS
	

Table 88: 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 + Assessment-lower* 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-2023-0687

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 89: CVE-2023-0687 References

Affected Components

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

Table 90: 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 91: 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 92: 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 93: CVE-2023-0687 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A	High
CVSS:2.0	NVD-CNA-NVD + Assessment	4.0	AV:A/AC:H/Au:S/C:P/I:P/A:P	Medium

Table 94: CVE-2023-0687 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	9.8	5.9	3.9	8.8	5.9
CVSS:2.0	NVD-CNA-NVD + Assessment	4.0	6.4	2.5		

Table 95: CVE-2023-0687 Context Severity Details

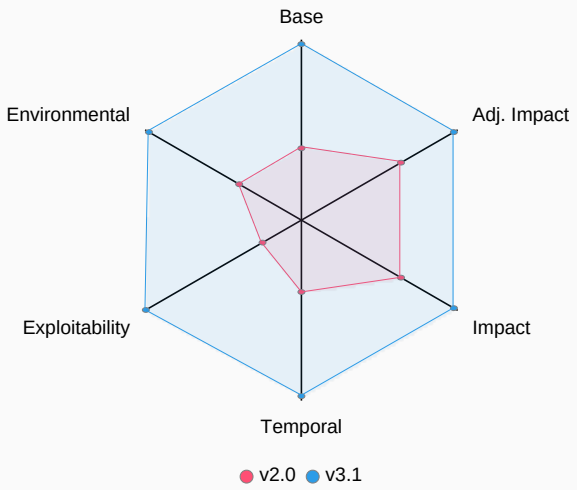
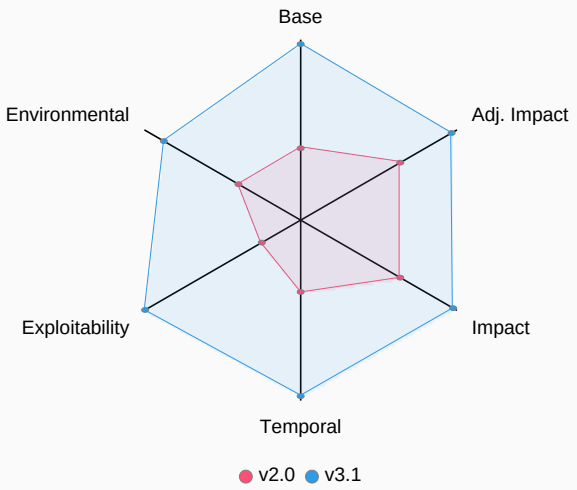
Initial CVSS	Context CVSS
	

Table 96: 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 + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A`
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 97: 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 98: 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 99: CVE-2022-41409 Initial Severity

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

Table 100: 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 101: CVE-2022-41409 Alerts

Assessment

Summary

Insignificant Due Medium

Context Severity

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

Table 102: CVE-2022-41409 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.5	3.6	3.9	6.5	3.6

Table 103: CVE-2022-41409 Context Severity Details

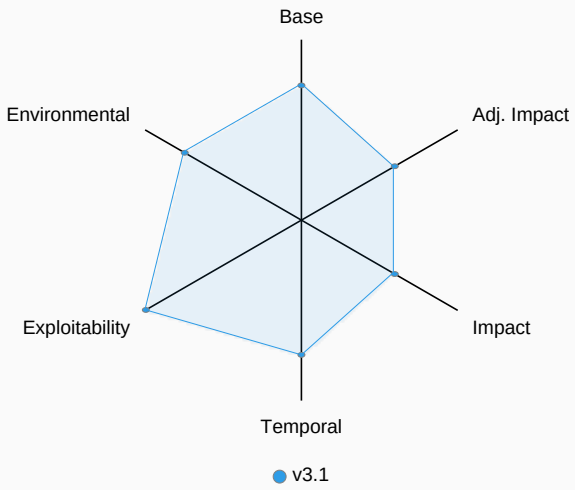
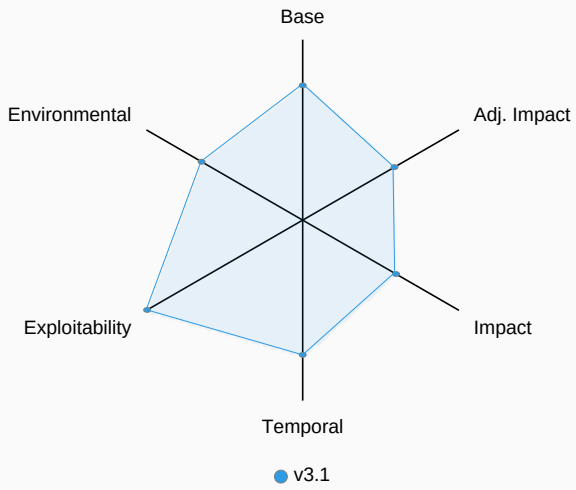
Initial CVSS	Context CVSS
	

Table 104: CVE-2022-41409 Severity Charts

Rationale
Score is below 7,0

Priority

Due (**7.5** from base score **6.5**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A`
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 105: 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 106: 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 107: CVE-2022-37832 Initial Severity

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

Table 108: 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 109: CVE-2022-37832 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A	High

Table 110: CVE-2022-37832 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	9.8	5.9	3.9	8.8	5.9

Table 111: CVE-2022-37832 Context Severity Details

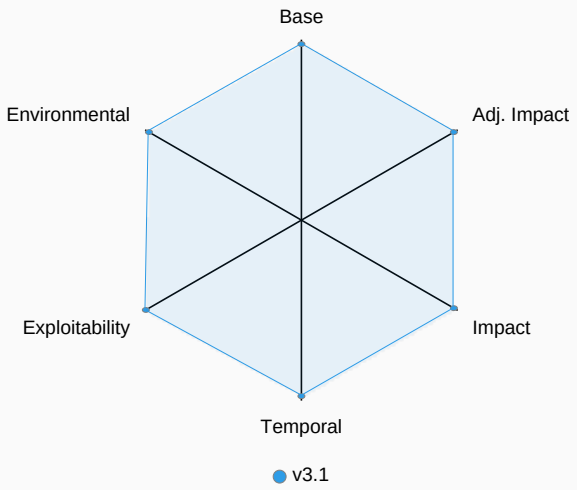
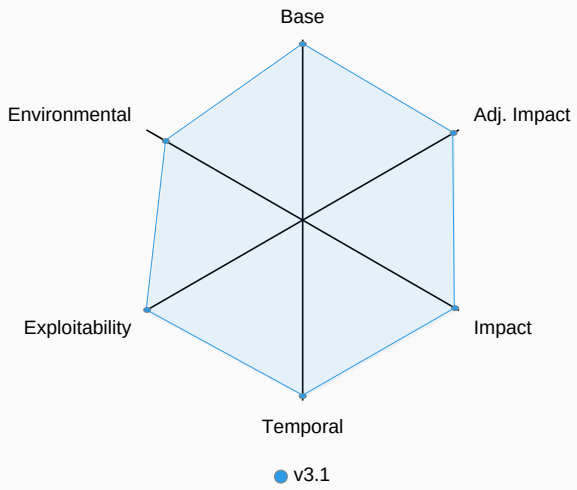
Initial CVSS	Context CVSS
	

Table 112: 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 + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A`
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 113: CVE-2022-37434 References

Affected Components

Component	Artifact Id	Version
zlib	`zlib-1.2.11`	`1.2.11`

Table 114: 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 115: CVE-2022-37434 Initial Severity

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

Table 116: CVE-2022-37434 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-cfmr-vrgj-vqwv	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 117: CVE-2022-37434 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.8	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A`	High

Table 118: CVE-2022-37434 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	9.8	5.9	3.9	8.8	5.9

Table 119: CVE-2022-37434 Context Severity Details

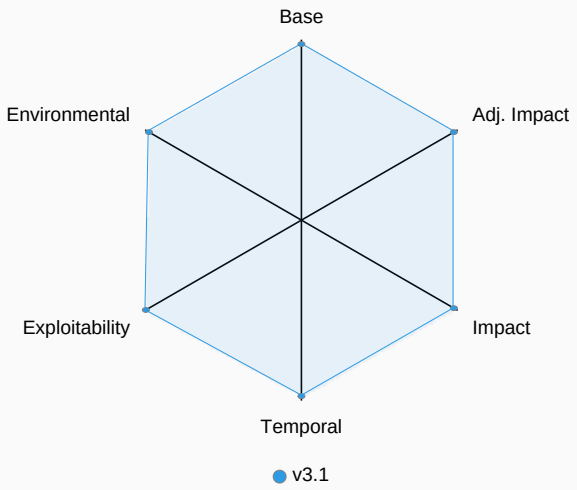
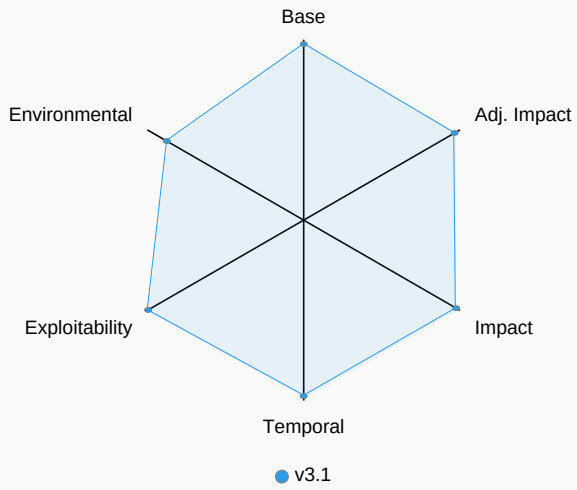
Initial CVSS	Context CVSS
	

Table 120: 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 + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A`
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 121: CVE-2022-35737 References

Affected Components

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

Table 122: 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 123: CVE-2022-35737 Initial Severity

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

Table 124: 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 125: CVE-2022-35737 Alerts

Assessment

Summary

Insignificant | Default | **Medium**

Context Severity

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

Table 126: CVE-2022-35737 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.5	3.6	3.9	6.5	3.6

Table 127: CVE-2022-35737 Context Severity Details

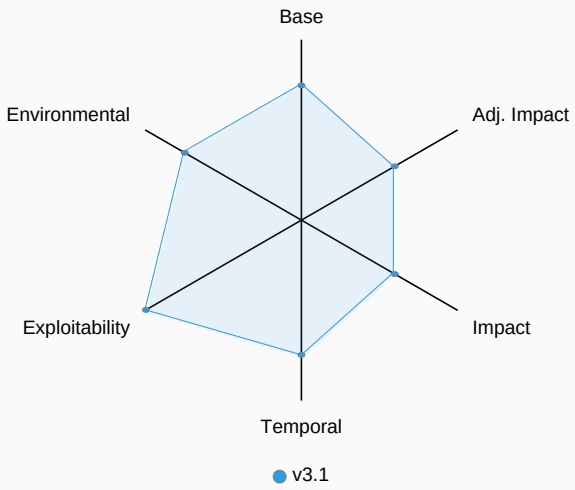
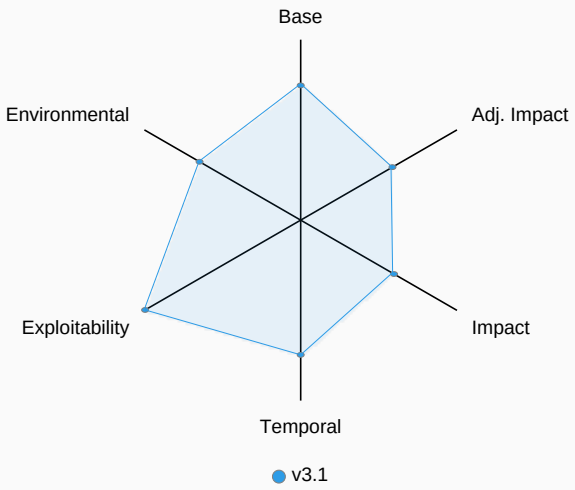
Initial CVSS	Context CVSS
	

Table 128: CVE-2022-35737 Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A`
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	sqlite (ver. 3) is still supported by it's 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 129: 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 130: 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 131: 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 132: 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 133: CVE-2022-29458 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	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 + Assessment	4.3	`AV:A/AC:M/Au:N/C:P/I:N/A:P`	Medium

Table 134: CVE-2022-29458 Context Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:3.1	NVD-CNA-NVD + Assessment	7.1	5.2	1.8

Scheme	Source	Base	Impact	Exploitability
CVSS:2.0	NVD-CNA-NVD + Assessment	4.3	4.9	5.5

Table 135: CVE-2022-29458 Context Severity Details

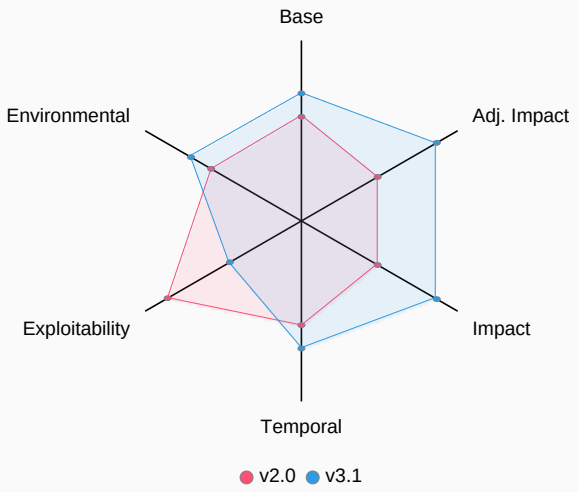
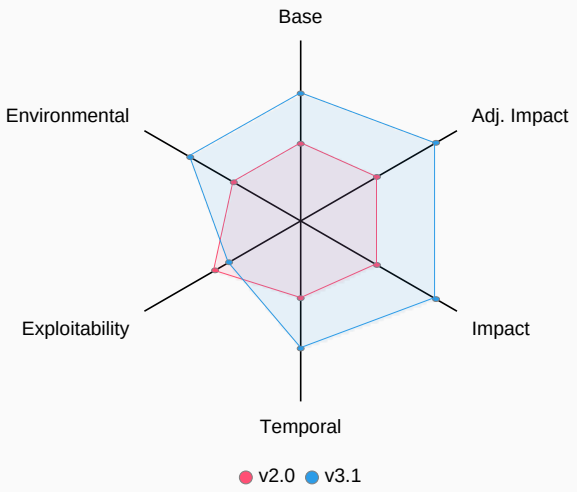
Initial CVSS	Context CVSS
	

Table 136: 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 + Assessment-lower* provides the vector: `CVSS:3.1/AV:L/AC:L/PR:N/UI:R/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-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 137: CVE-2022-23219 References

Affected Components

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

Table 138: 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 139: 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 140: 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 141: CVE-2022-23219 Alerts

Assessment

Summary

In Review Escalate High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A	High

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD + Assessment	5.8	AV:A/AC:L/Au:N/C:P/I:P/A:P	Medium

Table 142: CVE-2022-23219 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	9.8	5.9	3.9	8.8	5.9
CVSS:2.0	NVD-CNA-NVD + Assessment	5.8	6.4	6.5		

Table 143: CVE-2022-23219 Context Severity Details

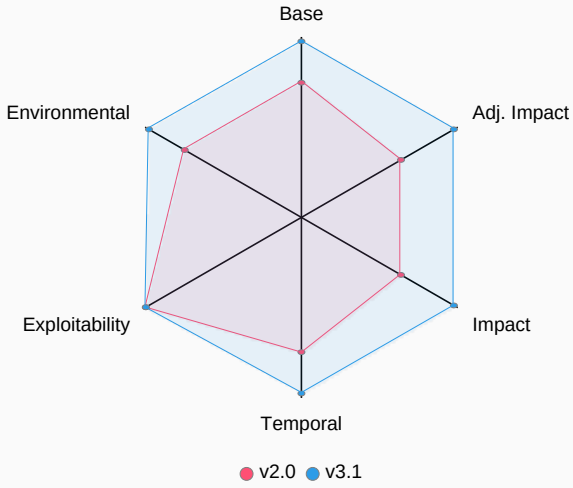
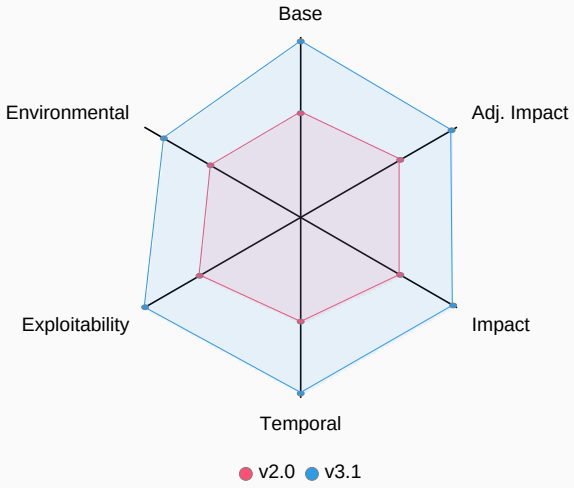
Initial CVSS	Context CVSS
	

Table 144: CVE-2022-23219 Severity Charts

Rationale
The vulnerability has automatically been marked as in review.

Priority

Escalate (**12.8** from base score **8.8**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A
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 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.

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

Table 145: CVE-2022-23218 References

Affected Components

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

Table 146: 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 147: 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 148: 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 149: CVE-2022-23218 Alerts

Assessment

Summary

In Review Escalate High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A	High
CVSS:2.0	NVD-CNA-NVD + Assessment	5.8	AV:A/AC:L/Au:N/C:P/I:P/A:P	Medium

Table 150: CVE-2022-23218 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	9.8	5.9	3.9	8.8	5.9
CVSS:2.0	NVD-CNA-NVD + Assessment	5.8	6.4	6.5		

Table 151: CVE-2022-23218 Context Severity Details

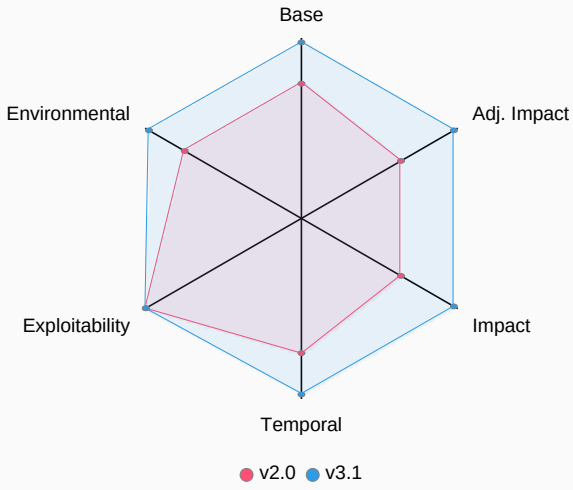
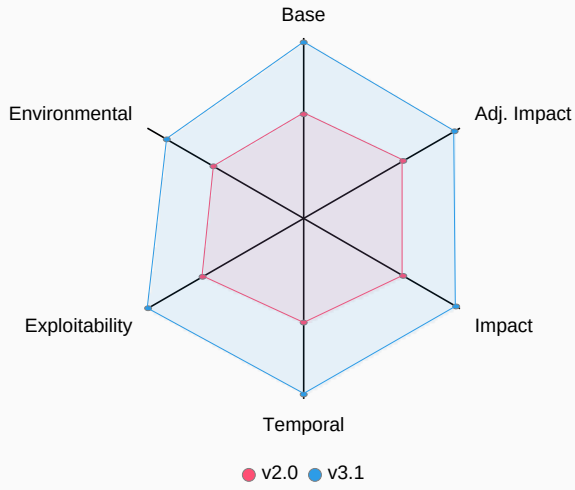
Initial CVSS	Context CVSS
	

Table 152: CVE-2022-23218 Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (**12.8** from base score **8.8**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A

Criteria	Explanation
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 ETYPE_OK 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 153: CVE-2021-46848 References

Affected Components

Component	Artifact Id	Version
libtasn1	`libtasn1-4.16.0`	`4.16.0`

Table 154: 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 155: CVE-2021-46848 Initial Severity

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

Table 156: 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 157: CVE-2021-46848 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/MAV:A	High

Table 158: CVE-2021-46848 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	9.1	5.2	3.9	8.1	5.2

Table 159: CVE-2021-46848 Context Severity Details

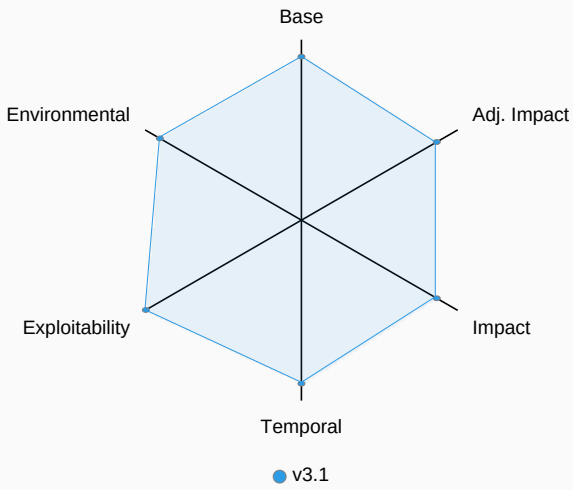
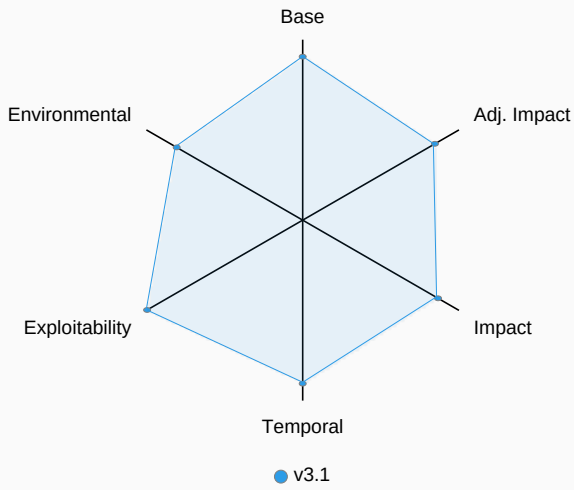
Initial CVSS	Context CVSS
	

Table 160: 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 + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/MAV:A
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 161: CVE-2021-43396 References

Affected Components

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

Table 162: 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 163: 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 164: 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 165: CVE-2021-43396 Alerts

Assessment

Summary

Insignificant Escalate Medium

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/MAV:A	Medium
CVSS:2.0	NVD-CNA-NVD + Assessment	3.3	AV:A/AC:L/Au:N/C:N/I:P/A:N	Low

Table 166: CVE-2021-43396 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.5	3.6	3.9	6.5	3.6
CVSS:2.0	NVD-CNA-NVD + Assessment	3.3	2.9	6.5		

Table 167: CVE-2021-43396 Context Severity Details

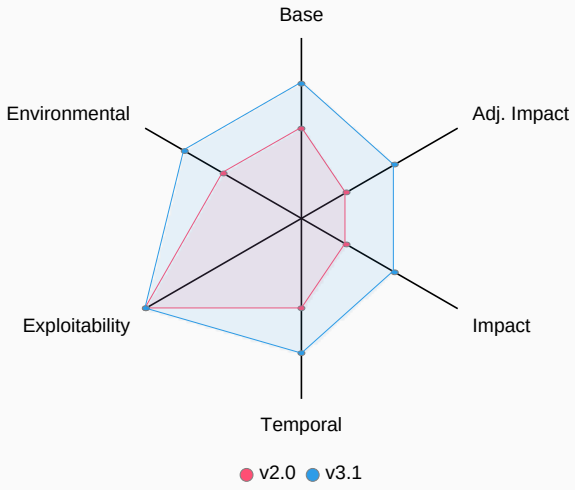
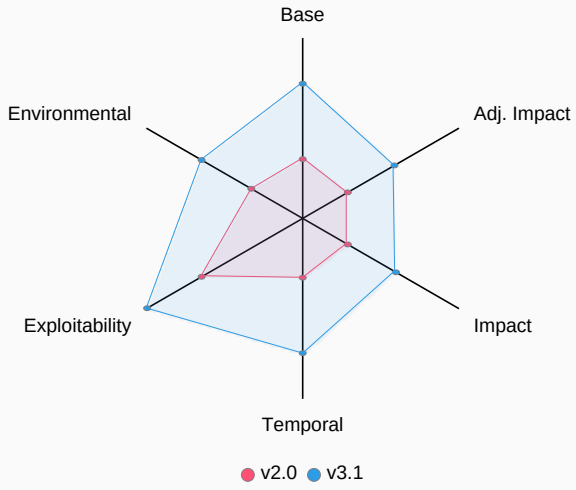
Initial CVSS	Context CVSS
	

Table 168: CVE-2021-43396 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 + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/MAV:A

Criteria	Explanation
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 169: CVE-2021-3998 References

Affected Components

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

Table 170: 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 171: CVE-2021-3998 Initial Severity

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

Table 172: 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 173: CVE-2021-3998 Alerts

Assessment

Summary

Insignificant | Default | Medium

Context Severity

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

Table 174: CVE-2021-3998 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.5	3.6	3.9	6.5	3.6

Table 175: CVE-2021-3998 Context Severity Details

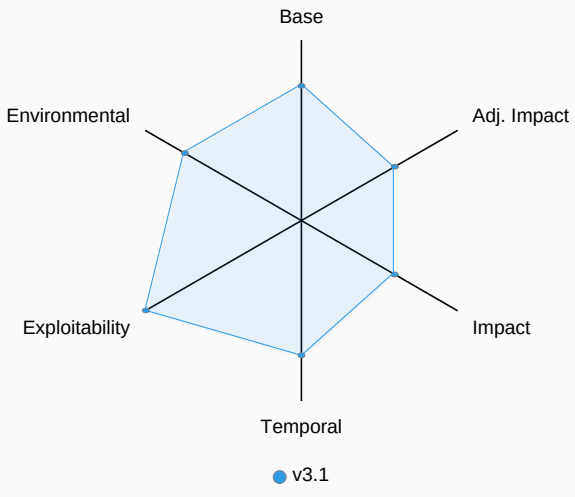
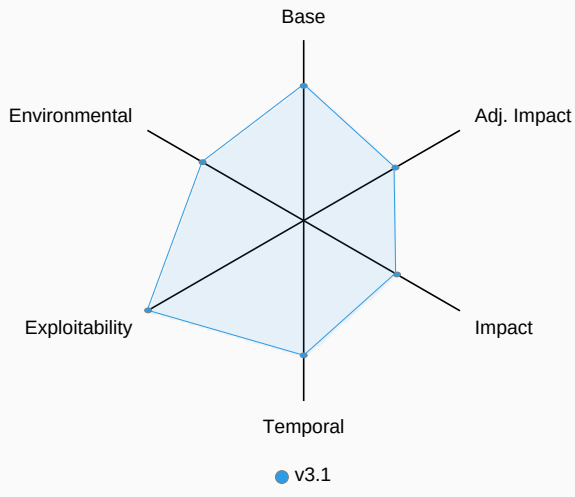
Initial CVSS	Context CVSS
	

Table 176: CVE-2021-3998 Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/MAV:A`
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_captoinfo in captoinfo.c has a heap-based buffer overflow.

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

Table 177: 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 178: 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 179: 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 180: 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_captoinfo in captoinfo.c has a heap-based buffer overflow.	2022-05-24	2022-05-24

Table 181: CVE-2021-39537 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/MAV:A	High
CVSS:2.0	NVD-CNA-NVD + Assessment	5.4	AV:A/AC:M/Au:N/C:P/I:P/A:P	Medium

Table 182: CVE-2021-39537 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	8.8	5.9	2.8	8.0	5.9
CVSS:2.0	NVD-CNA-NVD + Assessment	5.4	6.4	5.5		

Table 183: CVE-2021-39537 Context Severity Details

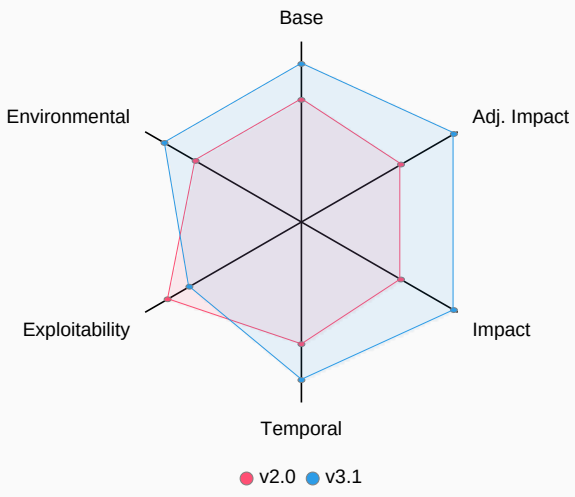
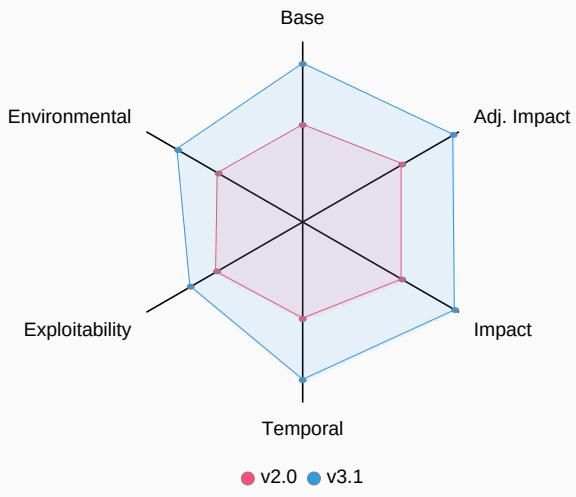
Initial CVSS	Context CVSS
	

Table 184: 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 + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/MAV:A`
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 185: CVE-2021-38604 References

Affected Components

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

Table 186: 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 187: 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 188: 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 189: CVE-2021-38604 Alerts

Assessment

Summary

Insignificant | Default | **Medium**

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A	Medium
CVSS:2.0	NVD-CNA-NVD + Assessment	3.3	AV:A/AC:L/Au:N/C:N/I:N/A:P	Low

Table 190: CVE-2021-38604 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.5	3.6	3.9	6.5	3.6
CVSS:2.0	NVD-CNA-NVD + Assessment	3.3	2.9	6.5		

Table 191: CVE-2021-38604 Context Severity Details

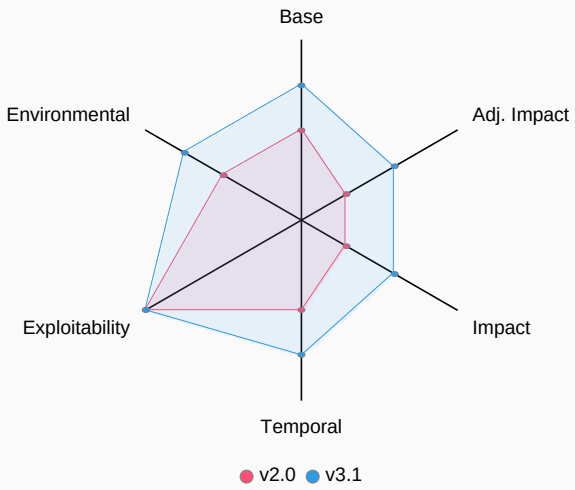
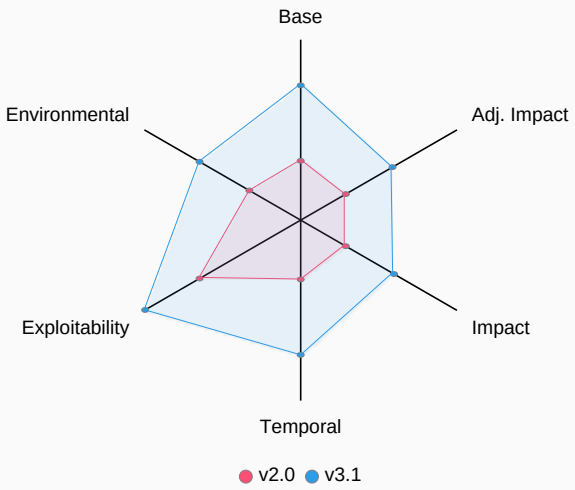
Initial CVSS	Context CVSS
	

Table 192: CVE-2021-38604 Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A`
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-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 193: CVE-2020-25638 References

Affected Components

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

Table 194: 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 195: 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 196: 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 197: CVE-2020-25638 Alerts

Assessment

Summary

Insignificant Escalate Medium

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	6.8	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/MAV:A	Medium
CVSS:2.0	NVD-CNA-NVD + Assessment	4.3	AV:A/AC:M/Au:N/C:P/I:P/A:N	Medium

Table 198: CVE-2020-25638 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.4	5.2	2.2	6.8	5.2
CVSS:2.0	NVD-CNA-NVD + Assessment	4.3	4.9	5.5		

Table 199: CVE-2020-25638 Context Severity Details

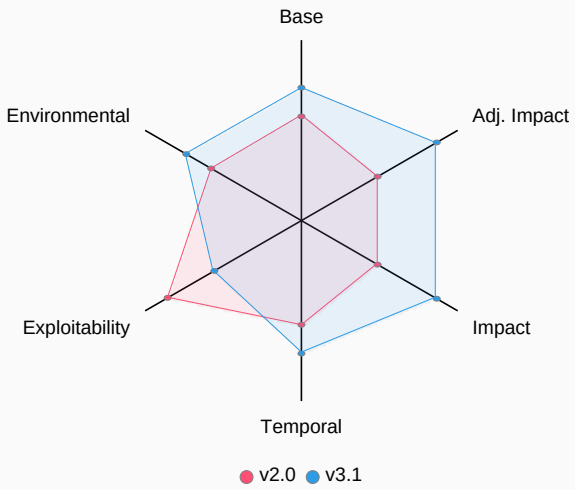
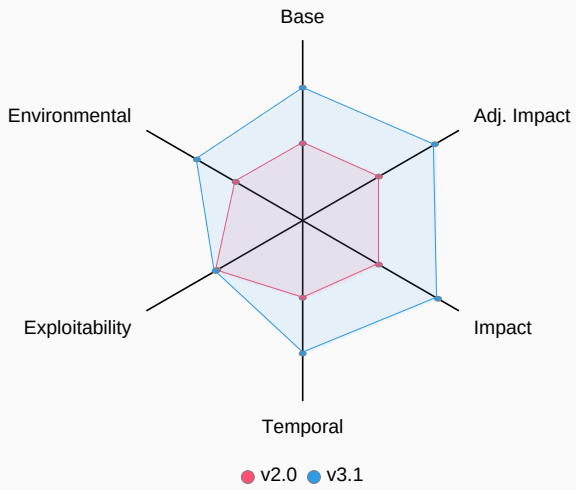
Initial CVSS	Context CVSS
	

Table 200: CVE-2020-25638 Severity Charts

Rationale
Score is below 7,0

Priority

Escalate (**9.8** from base score **6.8**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/MAV:A`
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 URIs 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 201: CVE-2020-13956 References

Affected Components

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

Table 202: 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 203: 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 204: 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 205: CVE-2020-13956 Alerts

Assessment

Summary

Insignificant Default Medium

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	4.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/MAV:A	Medium
CVSS:2.0	NVD-CNA-NVD + Assessment	3.3	AV:A/AC:L/Au:N/C:N/I:P/A:N	Low

Table 206: CVE-2020-13956 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	5.3	1.4	3.9	4.3	1.4
CVSS:2.0	NVD-CNA-NVD + Assessment	3.3	2.9	6.5		

Table 207: CVE-2020-13956 Context Severity Details

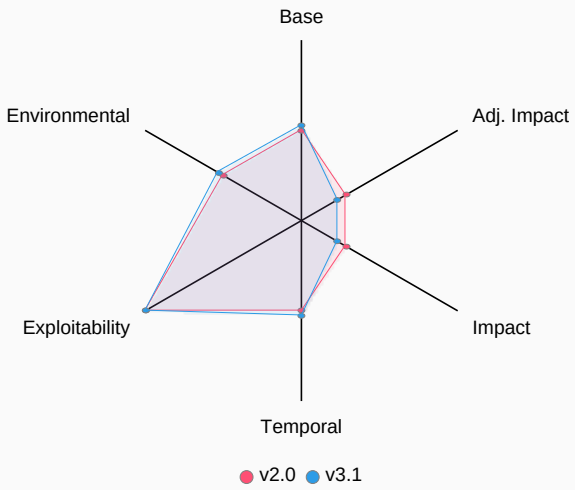
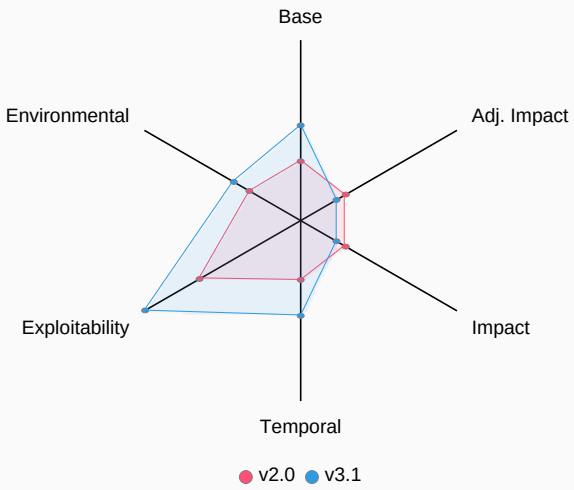
Initial CVSS	Context CVSS
	

Table 208: 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 + Assessment-lower* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/MAV:A`
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 209: 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-spi-3.8.5.jar	3.8.5
	io.quarkus.quarkus-hibernate-orm-deployment-3.8.5.jar	3.8.5

Table 210: 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 211: 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 212: 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 213: CVE-2019-14900 Alerts

Assessment

Summary

Insignificant | Due | Medium

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	5.7	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/MAV:A	Medium
CVSS:2.0	NVD-CNA-NVD + Assessment	2.7	AV:A/AC:L/Au:S/C:P/I:N/A:N	Low

Table 214: CVE-2019-14900 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	6.5	3.6	2.8	5.7	3.6
CVSS:2.0	NVD-CNA-NVD + Assessment	2.7	2.9	5.1		

Table 215: CVE-2019-14900 Context Severity Details

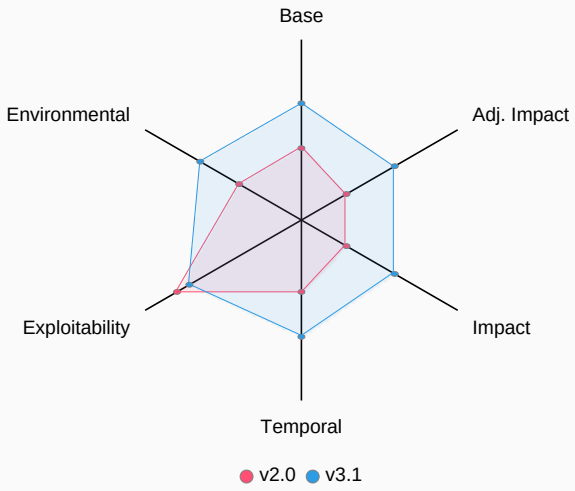
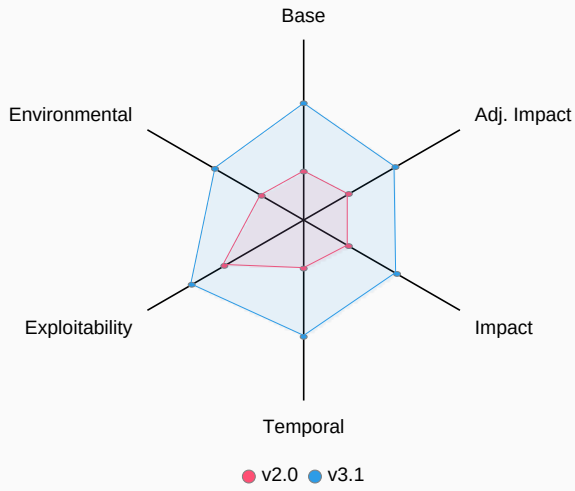
Initial CVSS	Context CVSS
	

Table 216: CVE-2019-14900 Severity Charts

Rationale
Score is below 7,0

Priority

Due (**8.7** from base score **5.7**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/MAV:A
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 217: CVE-2018-25032 References

Affected Components

Component	Artifact Id	Version
zlib	`zlib-1.2.11`	`1.2.11`

Table 218: 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 219: 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 220: 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 221: CVE-2018-25032 Alerts

Assessment

Summary

Insignificant | Default | **Medium**

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A	Medium
CVSS:2.0	NVD-CNA-NVD + Assessment	3.3	AV:A/AC:L/Au:N/C:N/I:N/A:P	Low

Table 222: CVE-2018-25032 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	7.5	3.6	3.9	6.5	3.6
CVSS:2.0	NVD-CNA-NVD + Assessment	3.3	2.9	6.5		

Table 223: CVE-2018-25032 Context Severity Details

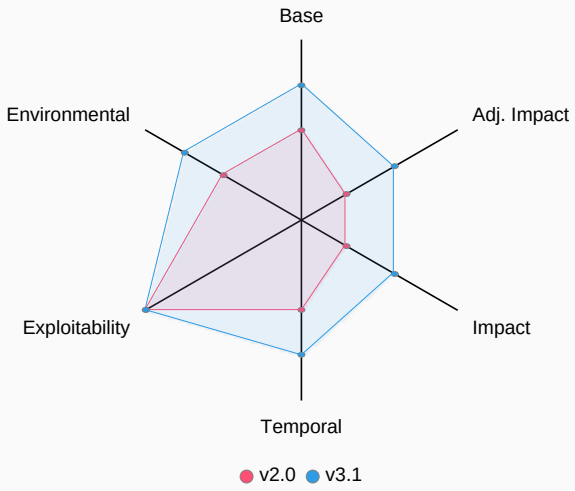
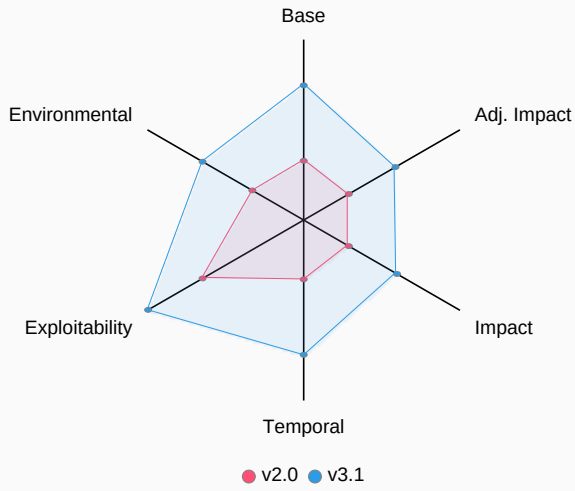
Initial CVSS	Context CVSS
	

Table 224: CVE-2018-25032 Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A
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 225: 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 226: 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 227: CVE-2018-15529 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	6.5	6.4	8.0

Table 228: CVE-2018-15529 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-9xfc-48gq-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 229: CVE-2018-15529 Alerts

Assessment

Summary

In Review | Default | High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	8.0	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/MAV:A	High
CVSS:2.0	NVD-CNA-NVD + Assessment	5.2	AV:A/AC:L/Au:S/C:P/I:P/A:P	Medium

Table 230: CVE-2018-15529 Context Severity

Scheme	Source	Base	Impact	Exploitability	Environmental	Adjusted impact
CVSS:3.1	NVD-CNA-NVD + Assessment	8.8	5.9	2.8	8.0	5.9
CVSS:2.0	NVD-CNA-NVD + Assessment	5.2	6.4	5.1		

Table 231: CVE-2018-15529 Context Severity Details

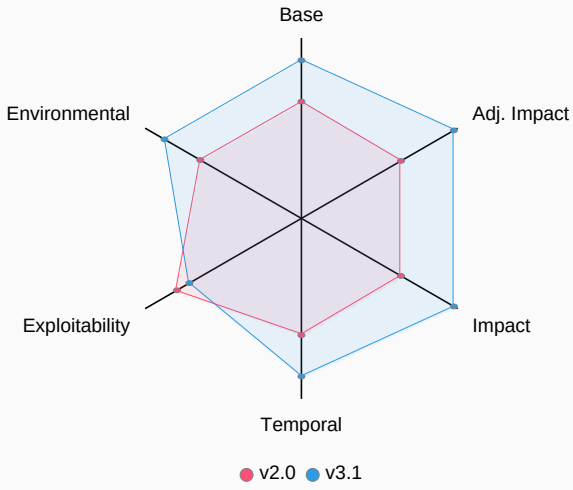
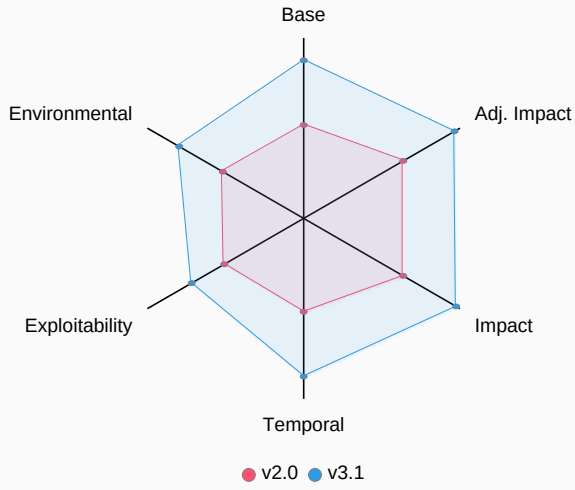
Initial CVSS	Context CVSS
	

Table 232: 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 + Assessment-lower* provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/MAV:A
Keywords	No keyword sets matched.

Criteria	Explanation
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-2016-7091

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 233: CVE-2016-7091 References

Affected Components

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

Table 234: 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 235: 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 236: 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 237: CVE-2016-7091 Alerts

Assessment

Summary

Insignificant Elevated Medium

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	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 + Assessment	4.9	AV:L/AC:L/Au:N/C:C/I:N/A:N	Medium

Table 238: CVE-2016-7091 Context Severity

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

Table 239: CVE-2016-7091 Context Severity Details

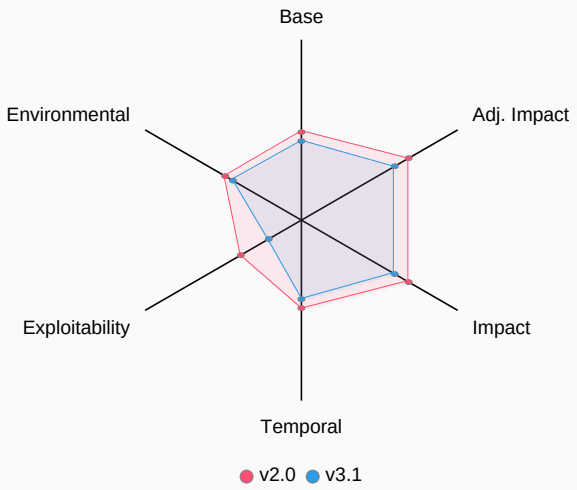
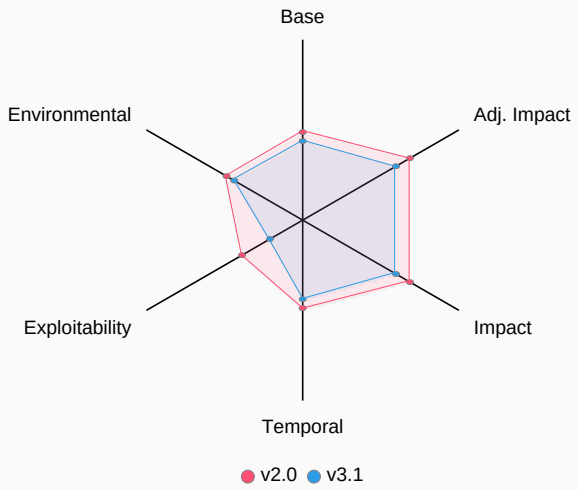
Initial CVSS	Context CVSS
	

Table 240: 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 + Assessment-lower* 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 241: CVE-2016-2781 References

Affected Components

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

Table 242: 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 243: 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 244: 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 245: CVE-2016-2781 Alerts

Assessment

Summary

Insignificant | Default | **Medium**

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD + Assessment	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 + Assessment	2.1	AV:L/AC:L/Au:N/C:N/I:P/A:N	Low

Table 246: CVE-2016-2781 Context Severity

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

Table 247: CVE-2016-2781 Context Severity Details

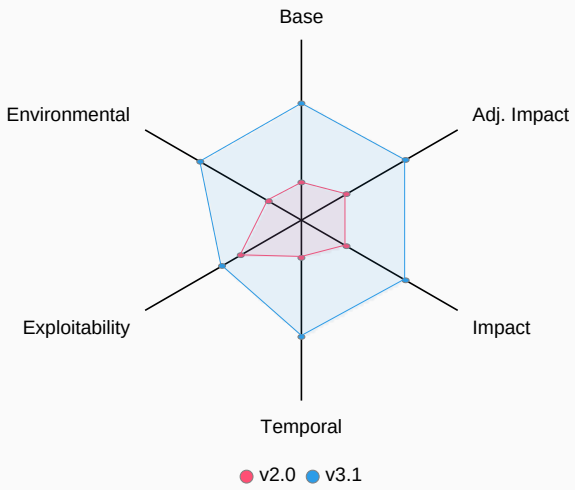
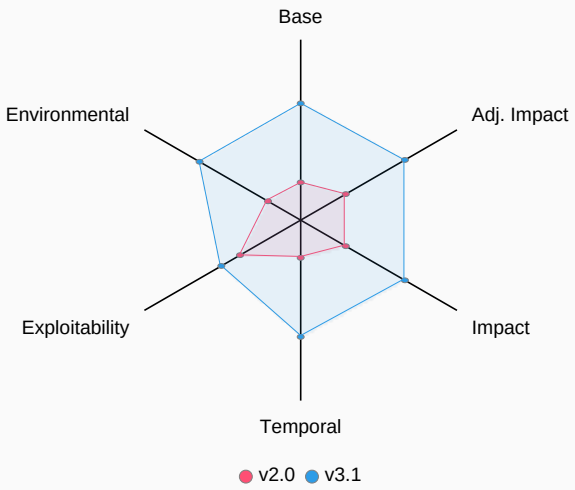
Initial CVSS	Context CVSS
	

Table 248: 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 + Assessment-lower* 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 249: 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 250: 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 251: CVE-2013-0136 Initial Severity

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

Table 252: 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 253: CVE-2013-0136 Alerts

Assessment

Summary

In Review Due High

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD + Assessment	7.4	AV:A/AC:M/Au:S/C:C/I:C/A:C	High

Table 254: CVE-2013-0136 Context Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:2.0	NVD-CNA-NVD + Assessment	7.4	10.0	4.4

Table 255: CVE-2013-0136 Context Severity Details

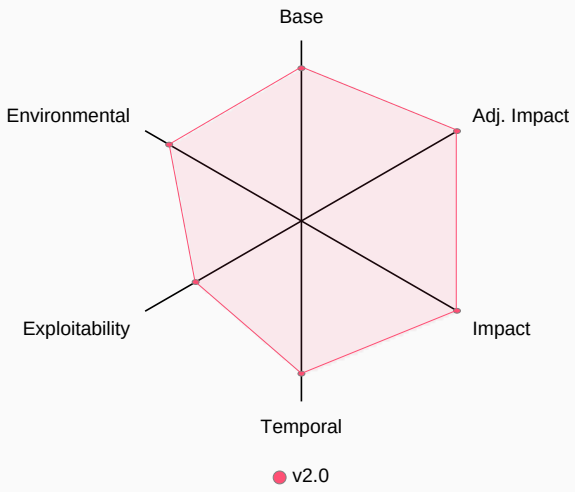
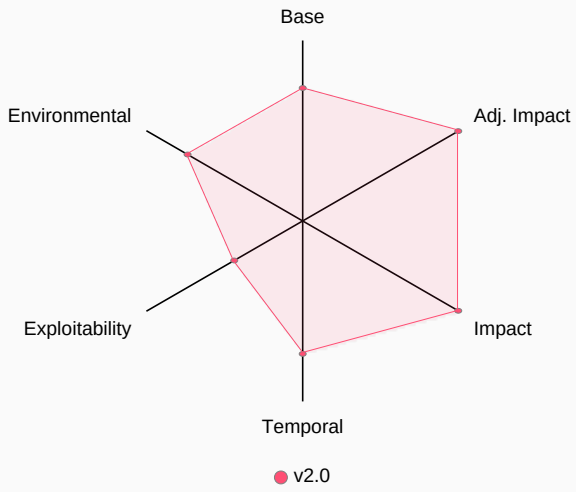
Initial CVSS	Context CVSS
	

Table 256: CVE-2013-0136 Severity Charts

Rationale
The vulnerability has automatically been marked as in review.

Priority

Due (**8.4** from base score **7.4**)

Criteria	Explanation
CVSS Overall	*CVSS:2.0 NVD-CNA-NVD + Assessment-lower* provides the vector: `AV:A/AC:M/Au:S/C:C/I:C/A:C`
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 257: CVE-2011-0536 References

Affected Components

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

Table 258: 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 259: CVE-2011-0536 Initial Severity

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

Table 260: 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 261: CVE-2011-0536 Alerts

Assessment

Summary

Insignificant | Default | **Medium**

Context Severity

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

Table 262: CVE-2011-0536 Context Severity

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

Table 263: CVE-2011-0536 Context Severity Details

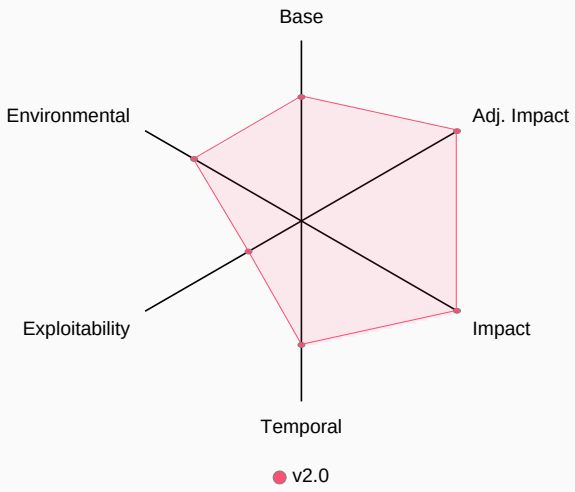
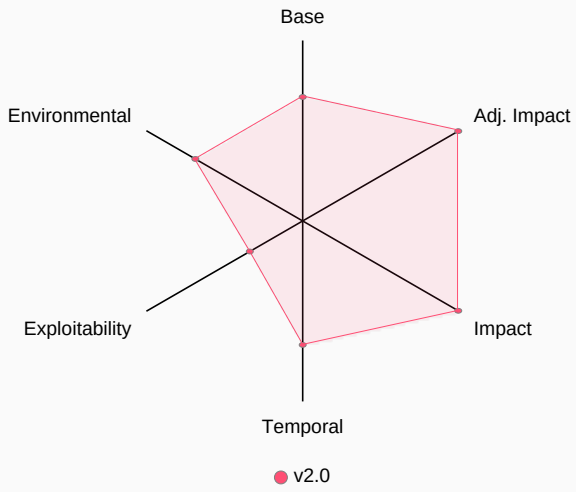
Initial CVSS	Context CVSS
	

Table 264: 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 + Assessment-lower* 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 265: CVE-2010-4756 References

Affected Components

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

Table 266: 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 267: CVE-2010-4756 Initial Severity

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

Table 268: CVE-2010-4756 Initial Severity Details

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-x2r9-jfjp-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 269: CVE-2010-4756 Alerts

Assessment

Summary

Insignificant Elevated Low

Context Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD + Assessment	2.7	`AV:A/AC:L/Au:S/C:N/I:N/A:P`	Low

Table 270: CVE-2010-4756 Context Severity

Scheme	Source	Base	Impact	Exploitability
CVSS:2.0	NVD-CNA-NVD + Assessment	2.7	2.9	5.1

Table 271: CVE-2010-4756 Context Severity Details

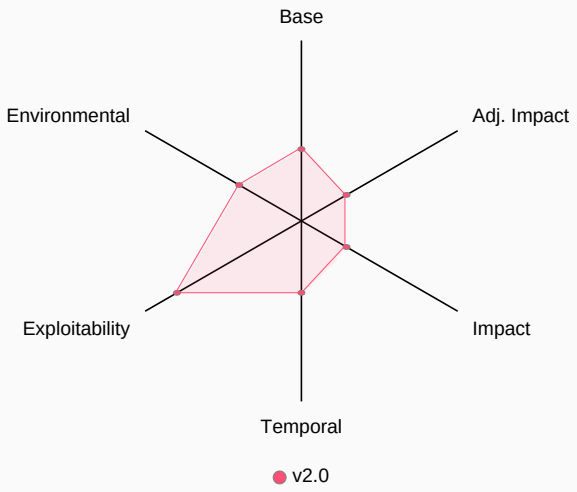
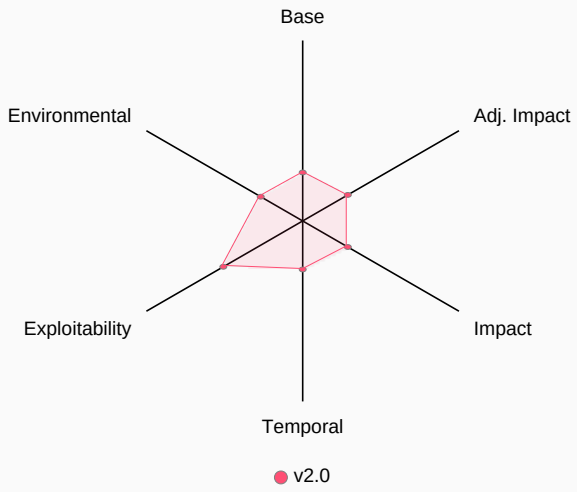
Initial CVSS	Context CVSS
	

Table 272: CVE-2010-4756 Severity Charts

Rationale
Score is below 7,0

Priority

Elevated (**3.7** from base score **2.7**)

Criteria	Explanation
CVSS Overall	*CVSS:2.0 NVD-CNA-NVD + Assessment-lower* provides the vector: `AV:A/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

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 State 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)*.