Doc. Identifier: \${document.id}

\${product.name} \${product.version}

\${document.name}

Doc. Identifier: \${document.id}

Doc. Version: \${document.version}

\${organization.name} \${organization.address}

Contents

1	ae-artifact-analysis Security Advisories	8
2	ae-artifact-analysis Affected Assets	. 8
3	ae-artifact-analysis Vulnerability Details	8
	CVE-2024-47535	
	CVE-2024-47772	
	CVE-2024-36124	_
	CVE-2023-45960	
	CVE-2023-44487	
	CVE-2023-41330	
	CVE-2023-37460	
	CVE-2023-3635	
	CVE-2023-34623	
	CVE-2023-34462	. 19
	CVE-2023-33953	. 20
	CVE-2023-32732	. 22
	CVE-2023-2976	. 23
	CVE-2023-28115	. 24
	CVE-2023-0833	. 25
	CVE-2022-44730	. 26
	CVE-2022-44729	. 28
	CVE-2022-4245	. 29
	CVE-2022-4244	
	CVE-2022-41881	
	CVE-2022-34169	
	CVE-2022-24823	
	CVE-2022-1271	
	CVE-2021-43797	
	CVE-2021-4277	
	CVE-2021-37137	
	CVE-2021-37136	
	CVE-2021-35939	
	CVE-2021-35938	
	CVE-2021-35937	
	CVE-2021-3521	_
	CVE-2021-3421	
	CVE-2021-33813	
	CVE-2021-26291	
	CVE-2021-25738	
	CVE-2021-24028	_
	CVE-2021-21409	
	CVE-2021-21295	
	CVE-2021-21290	
	CVE-2021-20266	
	CVE-2020-8908	
	CVE-2020-8570	
	CVE-2020-8554	
	CVE-2020-7768	
	♥ ₹ ₹ ZUZU - 1 ĴĴĴĴ	. 04

CVE-2020-13936	65
CVE-2020-10683	66
CVE-2020-10519	67
CVE-2020-10518	69
CVE-2020-10517	
CVE-2019-3565	
CVE-2019-3564	
CVE-2019-3559.	
CVE-2019-3558	
CVE-2019-3553	
CVE-2019-3552	
CVE-2019-20445	
CVE-2019-20444	
CVE-2019-16869	
CVE-2019-11939	
CVE-2019-11938	
CVE-2019-10086	
CVE-2018-6969	87
CVE-2018-1000632	88
CVE-2017-9530	90
CVE-2017-9431	91
CVE-2017-8359	92
CVE-2017-7861	
CVE-2017-7860	
CVE-2017-7501	
CVE-2017-1000487	
CVE-2016-7080	
CVE-2016-7000	
CVE-2016-5328	
CVE-2015-5191	
CVE-2015-4035	
CVE-2015-2156	
CVE-2014-8118	
CVE-2014-4200	
CVE-2014-4199	
CVE-2014-3488	
CVE-2014-0114	
CVE-2013-6435	111
CVE-2012-2055	112
CVE-2012-0815	114
CVE-2012-0061	115
CVE-2012-0060	116
CVE-2011-3378	118
CVE-2010-2199	119
CVE-2010-2198.	
CVE-2010-2197	
CVE-2010-2059.	
CVE-2009-3014	
CVE-2009-3010.	
CVE-2009-3010	
CVE-2009-1251	
CVE-2008-2503	
CVE-2008-2298	
CVE-2008-0501	
CVE-2007-6640	
CVE-2007-4039	
CVE-2007-1794	
CVE-2007-1466	
CVE 2007 1157	127

CVE 2007 1127		38
	14	
	14	
CVE-2006-0496	14	43
CVE-2005-4889		44
CVE-2005-4837	14	46
	14	
CVE-2005-2266	15	53
CVE-2005-2265	15	54
CVE-2005-2263	1£	55
	15	
	16	
CVE-2005-1159	16	63
CVE-2005-1157		64
CVE-2005-0590		72
CVE-2005-0588		74
CVE-2005-0586		75
CVF-2005-0585		76
	17	
		-
	18	
CVE-2005-0147	18	83
CVE-2005-0146	18	84
CVE-2005-0144	18	85
CVE-2005-0143	18	86
		_
CVE-2004-1381		93
CVE-2004-1380		94
CVE-2004-1316	19	95
CVE-2004-1156		96
	20	
CVE-2004-0903		04
CVE 0004 0000	^^	$^{\circ}$

CVE-2004-0765	
CVE-2004-0764	
CVE-2004-0762	209
CVE-2004-0761	210
CVE-2004-0760	211
CVE-2004-0759	212
CVE-2004-0758	213
CVE-2004-0757	214
CVE-2004-0478	216
CVE-2002-2364	217
CVE-2002-2362	
CVE-2002-0815	
CVE-2001-0234	
CVE-2000-0655	
CVE-1999-0377	
4 ae-artifact-analysis Affected Components	224
juniversalchardet	
Caffeine cache	
uri-template	
jackson-coreutils-equivalence	
msg-simple	
json-schema-core	
,	
btf	
jackson-coreutils	
json-schema-validator	
JSONLD Java :: Core	
PortEx	
zstd-jni	
Package URL	
curvesapi	
Guava InternalFutureFailureAccess and InternalFutures	
OkHttp	
Okio	
Fabric8 :: Kubernetes :: Java Client API	
Fabric8 :: Kubernetes :: HttpClient :: OkHttp	
Fabric8:: Kubernetes Model:: Admission Registration, Authentication and Authorization	234
Fabric8 :: Kubernetes Model :: API Extensions	235
Fabric8 :: Kubernetes Model :: Apps	235
Fabric8 :: Kubernetes Model :: Autoscaling	235
Fabric8 :: Kubernetes Model :: Batch	236
Fabric8 :: Kubernetes Model :: Certificates	236
Fabric8 :: Kubernetes Model :: Common	237
Fabric8 :: Kubernetes Model :: Coordination	237
Fabric8 :: Kubernetes Model :: Core	
Fabric8 :: Kubernetes Model :: Discovery	
Fabric8 :: Kubernetes Model :: Events	
Fabric8 :: Kubernetes Model :: Extensions	
Fabric8 :: Kubernetes Model :: FlowControl	
Fabric8 :: Kubernetes Model :: Sigs :: Gateway API	
Fabric8 :: Kubernetes Model :: Metrics	
Fabric8 :: Kubernetes Model :: Networking	
Fabric8 :: Kubernetes Model :: Node	
Fabric8 :: Kubernetes Model :: Policy	
Fabric8 :: Kubernetes Model :: RBAC	
Fabric8 :: Kubernetes Model :: Resource	
Fabric8 :: Kubernetes Model :: Scheduling	
Fabric8 :: Kubernetes Model :: Storage Class	242

io.grpc:grpc-netty	
Netty/Common	
Netty/Transport/Native/Unix/Common	
CDI APIs	
JTidy	
Lucene Common Analyzers	
Lucene Memory	
Lucene Core	
Lucene Queries	
Lucene QueryParsers	
Lucene Sandbox	
Doxia :: Core	
Doxia Sitetools :: Decoration Model	
Doxia Sitetools :: Integration Tools	
Doxia :: Logging API	
Doxia :: XHTML5 Module	
Doxia :: XHTML Module	
Doxia :: Sink API	
Doxia Sitetools :: Site Renderer	
Doxia Sitetools :: Skin Model	
Maven Plugin Tools Java 5 Annotations	
Maven Plugin Tool for Java with Annotations	
Mayen Plugin Tools Extractor API	
Mayon Plugin Tools Generators	
Maven Plugin Tool for Java with Javadoc Tags	
Mayen Plugin Plugin	
Apache Mayon Reporting Implementation	
Apache Mayon Wagon y ARI	
Apache Maven Wagon :: API Maven Aether Provider	
Mayon Compat	
Mayon Corp	
Mayon Model Builder	
Maven Model Builder	
Maven Plugin API	
Maven Repository Metadata Model	
Maven Settings Builder	
Maven Settings	
Apache Thrift	
VelocityTools	
\${project.groupId}:\${project.artifactId}	
Plexus Common Utilities	
Plexus Archiver Component	
snappy	
JDOM	
Mozilla Rhino	
XZ for Java	
Xalan Java Serializer	
ae-artifact-analysis Vulnerability Notice	272
Con outifort analysis Vulnerability List	070
ae-artifact-analysis Vulnerability List	
Applicable	
In Review	
Not Applicable	
Incignificant	201

\${organization.name}	\${document.classification_en}	\${product.watermark.name}
Void		290

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi} Page 7 of 290 Doc. Date: \${document.date_

1 ae-artifact-analysis Security Advisories

The following security advisories have been detected for the query period.

New Security Advisories

No security advisories are present in the query period that are considered new in this context and have not yet been considered during vulnerability assessments.

Security Advisories in Review

No security advisories are present in the query period that are currently under review.

Reviewed Security Advisories

No security advisories are present in the query period that have already been considered in the assessment of the related vulnerabilities.

Not relevant Security Advisories

No security advisories are present in the query period that are considered irrelevant in this context.

Security Advisories Summary

There are no security advisories that are not present in the query period, but were matched by the affected components.

2 ae-artifact-analysis Affected Assets

No affected assets have been identified.

3 ae-artifact-analysis Vulnerability Details

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

CVE-2024-47535

Description

Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crashes. This vulnerability is fixed in 4.1.115.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2024-47535

Affected Assets

Asset Name	Asset Type	Asset Version
	composite	

Affected Components

Component	Artifact Id	Version
Netty/Common	netty-common-4.1.110.Final.jar	4.1.110.Final

Weakness

CWE-400

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:4.0	GitHub, Inc.	7.0	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:H/SI:H/SA:L/E:P	High
CVSS:3.1	GitHub, Inc.	5.5	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-xq3w-v528-46rv	Denial of Service attack on windows app using netty	2024-11-12	2024-11-12

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}

Criteria	Explanation	
CVSS Overall	verall CVSS:4.0 GitHub, Inc. provides the vector: CVSS:4.0 /AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:H/SI:H/SA:L/E:P	
Keywords No keyword sets matched.		
EPSS This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 89.63 % of all scored vulnerabilities.		
KEV This vulnerability has not been confirmed to have been exploited in the wild.		
EOL No end-of-life (EOL) information available.		
Assessment	The vulnerability status is in review .	

CVE-2024-45772

Description

Descrialization of Untrusted Data vulnerability in Apache Lucene Replicator. This issue affects Apache Lucene's replicator module: from 4.4.0 before 9.12.0. The deprecated org.apache.lucene.replicator.http package is affected. The org.apache.lucene.replicator.nrt package is not affected. Users are recommended to upgrade to version 9.12.0, which fixes the issue. Java serialization filters (such as -Djdk.serialFilter='!*' on the commandline) can mitigate the issue on vulnerable versions without impacting functionality.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2024-45772

Affected Components

Component	Artifact Id	Version
Lucene Common Analyzers	lucene-analyzers-common-8.11.2.jar	8.11.2
Lucene Memory	lucene-backward-codecs-8.11.2.jar	8.11.2
Lucene Core	lucene-core-8.11.2.jar	8.11.2
Lucene Queries	lucene-queries-8.11.2.jar	8.11.2
Lucene QueryParsers	lucene-queryparser-8.11.2.jar	8.11.2
Lucene Sandbox	lucene-sandbox-8.11.2.jar	8.11.2

Weakness

CWE-502

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	8.0	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	High

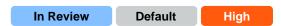
Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-g643-xq6w-r67c	Deserialization of Untrusted Data vulnerability in Apache Lucene Replicator.	2024-09-30	2024-09-30

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

\${document.name} Doc. Version: \${document.versi} Page 10 of 290 Doc. Date: \${document.date_

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2024-36124

Description

iq80 Snappy is a compression/decompression library. When uncompressing certain data, Snappy tries to read outside the bounds of the given byte arrays. Because Snappy uses the JDK class `sun.misc.Unsafe` to speed up memory access, no additional bounds checks are performed and this has similar security consequences as out-of-bounds access in C or C++, namely it can lead to non-deterministic behavior or crash the JVM. iq80 Snappy is not actively maintained anymore. As quick fix users can upgrade to version 0.5.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2024-36124

Affected Components

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

Weakness

CWE-125

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	GitHub, Inc.	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	Medium

Advisories

Doc. Identifier: \${document.id}

Alerts

ld	Summary	Create Date	Update Date
GHSA-8wh2-6qhj-h7j9	iq80 Snappy out-of-bounds read when uncompressing data, leading to JVM crash	2024-06-04	2024-06-04

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 GitHub, Inc. provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 89.63 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2023-45960

Description

Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-45960

Affected Components

Component	Artifact Id	Version
	dom4j-1.6.1.jar	1.6.1

Initial Severity

The vulnerability does not provide any CVSS severity information.

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-fgq9-fc3q-vqmw	Withdrawn Advisory: dom4j XML Entity Expansion vulnerability	2023-10-25	2023-10-25

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	No CVSS vector available.
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 end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2023-44487

Description

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-44487

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0
	ae-artifact-flow-grpc-0.135.0.jar	0.135.0

Weakness

CWE-400

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:4.0	GitHub, Inc.	6.9	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N	Medium
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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-qppj-fm5r-hxr3	HTTP/2 Stream Cancellation Attack	2023-10-10	2023-10-10
CERT-EU-2023-074	HTTP/2 Rapid Reset DDoS Vulnerability	2023-10-17	2023-10-17

Assessment

Summary

Insignificant Escalate Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Escalate (10.4 from base score 6.9)

Criteria	Explanation
CVSS Overall	CVSS:4.0 GitHub, Inc. provides the vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 83.78 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 1.42 % of all scored vulnerabilities.
KEV	This vulnerability, affecting IETF HTTP/2, has been confirmed to have been exploited in the wild. Summary: HTTP/2 Rapid Reset Attack 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://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/; https://nvd.nist.gov/vuln/detail/CVE-2023-44487 Due Date: 2023-10-31 Publish Date: 2023-10-10
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2023-41330

Doc. Identifier: \${document.id}

Description

knplabs/knp-snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. ## Issue On March 17th the vulnerability CVE-2023-28115 was disclosed, allowing an attacker to gain remote code execution through PHAR deserialization. Version 1.4.2 added a check `if (\strpos(\filename, 'phar://') === 0)` in the `prepareOutput` function to resolve this CVE, however if the user is able to control the second parameter of the `generateFromHtml()` function of Snappy, it will then be passed as the `filename` parameter in the `prepareOutput()` function. In the original vulnerability, a file name with a `phar://` wrapper could be sent to the `fileExists()` function, equivalent to the `file_exists()` PHP function. This allowed users to trigger a deserialization on arbitrary PHAR files. To fix this issue, the string is now passed to the `strpos()` function and if it starts with `phar://`, an exception is raised. However, PHP wrappers being case insensitive, this patch can be bypassed using `PHAR://` instead of `phar://`. A successful exploitation of this vulnerability allows executing

arbitrary code and accessing the underlying filesystem. The attacker must be able to upload a file and the server must be running a PHP version prior to 8. This issue has been addressed in commit `d3b742d61a` which has been included in version 1.4.3. Users are advised to upgrade. Users unable to upgrade should ensure that only trusted users may submit data to the `AbstractGenerator->generate(...)` function.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-41330

Affected Components

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

Weakness

CWE-502

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-92rv-4j2h-8mjj	Snappy PHAR deserialization vulnerability	2023-09-08	2023-09-08

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.76 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 11.54 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.

Criteria	Explanation
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2023-37460

Description

Plexis Archiver is a collection of Plexus components to create archives or extract archives to a directory with a unified `Archiver`/UnArchiver` API. Prior to version 4.8.0, using AbstractUnArchiver for extracting an archive might lead to an arbitrary file creation and possibly remote code execution. When extracting an archive with an entry that already exists in the destination directory as a symbolic link whose target does not exist - the `resolveFile()` function will return the symlink's source instead of its target, which will pass the verification that ensures the file will not be extracted outside of the destination directory. Later `Files.newOutputStream()`, that follows symlinks by default, will actually write the entry's content to the symlink's target. Whoever uses plexus archiver to extract an untrusted archive is vulnerable to an arbitrary file creation and possibly remote code execution. Version 4.8.0 contains a patch for this issue.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-37460

Affected Components

Component	Artifact Id	Version
Plexus Archiver Component	plexus-archiver-4.5.0.jar	4.5.0

Weakness

CWE-22

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-wh3p-fphp-9h2m	Arbitrary File Creation in AbstractUnArchiver	2023-07-25	2023-07-25

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

\${document.name} Doc. Version: \${document.versi} Page 16 of 290 Doc. Date: \${document.date_

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.36 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 13.25 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2023-3635

Description

GzipSource does not handle an exception that might be raised when parsing a malformed gzip buffer. This may lead to denial of service of the Okio client when handling a crafted GZIP archive, by using the GzipSource class.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-3635

Affected Components

Component	Artifact Id	Version
Okio	okio-1.17.2.jar	1.17.2

Weakness

CWE-195, CWE-681

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-w33c-445m-f8w7	Okio Signed to Unsigned Conversion Error vulnerability	2023-07-12	2023-07-12

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.08 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 63.76 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2023-34623

Description

An issue was discovered jtidy thru r938 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-34623

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-fv2r-hw24-8rxj	An issue was discovered jtidy thru r938 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	2023-06-14	2023-06-14

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versions}Page 18 of 290Doc. Date: \${document.date_

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.06 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 74.70 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2023-34462

Description

Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. The `SniHandler` can allocate up to 16MB of heap for each channel during the TLS handshake. When the handler or the channel does not have an idle timeout, it can be used to make a TCP server using the `SniHandler` to allocate 16MB of heap. The `SniHandler` class is a handler that waits for the TLS handshake to configure a `SslHandler` according to the indicated server name by the `ClientHello` record. For this matter it allocates a `ByteBuf` using the value defined in the `ClientHello` record. Normally the value of the packet should be smaller than the handshake packet but there are not checks done here and the way the code is written, it is possible to craft a packet that makes the `SslClientHelloHandler`. This vulnerability has been fixed in version 4.1.94.Final.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-34462

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-400, CWE-770

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:N/I:N/A:H	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-6mjq-h674-j845	netty-handler SniHandler 16MB allocation	2023-06-20	2023-06-20

Assessment

Summary

Incignificant	Default	Medium
Insignificant	Detault	wealum

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.12 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 52.00 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2023-33953

Description

gRPC contains a vulnerability that allows hpack table accounting errors could lead to unwanted disconnects between clients and servers in exceptional cases/ Three vectors were found that allow the following DOS attacks: - Unbounded memory buffering in the HPACK parser - Unbounded CPU consumption in the HPACK parser The unbounded CPU consumption is down to a copy that occurred per-input-block in the parser, and because that could be unbounded due to the memory copy bug we end up with an O(n^2) parsing loop, with n selected by the client. The unbounded memory buffering bugs: - The header size limit check was behind the string reading code, so we needed to first buffer up to a 4 gigabyte string before rejecting it as longer than 8 or 16kb. - HPACK varints have an encoding quirk whereby an infinite number of 0's can be added at the start of an integer. gRPC's hpack parser needed to read all of them before concluding a parse. - gRPC's metadata overflow check was performed per frame, so that the following sequence of frames could cause infinite buffering: HEADERS: containing a: 1 CONTINUATION: containing a: 2 CONTINUATION: containing a: 3 etc...

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-33953

Affected Components

Component	Artifact Id	Version
	ae-artifact-flow-grpc-0.135.0.jar	0.135.0

Weakness

CWE-789, CWE-770

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-496j-2rq6-j6cc	Excessive Iteration in gRPC	2023-08-09	2023-08-09

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.08 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 66.10 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2023-32732

Description

gRPC contains a vulnerability whereby a client can cause a termination of connection between a HTTP2 proxy and a gRPC server: a base64 encoding error for `-bin` suffixed headers will result in a disconnection by the gRPC server, but is typically allowed by HTTP2 proxies. We recommend upgrading beyond the commit in https://github.com/grpc/grpc/pull/32309 https://www.google.com/url

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-32732

Affected Components

Component	Artifact Id	Version
	ae-artifact-flow-grpc-0.135.0.jar	0.135.0

Weakness

CWE-440

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:N/A:L	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-9hxf-ppjv-w6rq	gRPC connection termination issue	2023-07-06	2023-07-06

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

Criteria	Explanation
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.10 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 57.07 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2023-2976

Description

Use of Java's default temporary directory for file creation in `FileBackedOutputStream` in Google Guava versions 1.0 to 31.1 on Unix systems and Android Ice Cream Sandwich allows other users and apps on the machine with access to the default Java temporary directory to be able to access the files created by the class. Even though the security vulnerability is fixed in version 32.0.0, we recommend using version 32.0.1 as version 32.0.0 breaks some functionality under Windows.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-2976

Affected Components

Component	Artifact Id	Version
Guava InternalFutureFailureAccess and InternalFutures	failureaccess-1.0.2.jar	1.0.2

Weakness

CWE-552

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-7g45-4rm6-3mm3	Guava vulnerable to insecure use of temporary directory	2023-06-14	2023-06-14

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 82.86 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2023-28115

Description

Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file_exists()` function. If an attacker can upload files of any type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-28115

Affected Components

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

Weakness

CWE-502

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-gq6w-q6wh-jggc	PHAR deserialization allowing remote code execution	2023-03-17	2023-03-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

	•
Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.56 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 9.41 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2023-0833

Description

A flaw was found in Red Hat's AMQ-Streams, which ships a version of the OKHttp component with an information disclosure flaw via an exception triggered by a header containing an illegal value. This issue could allow an authenticated attacker to access information outside of their regular permissions.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-0833

Affected Components

Component	Artifact Id	Version
OkHttp	okhttp-3.14.9.jar	3.14.9

Weakness

CWE-209

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versi}Page 25 of 290Doc. Date: \${document.date_

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.5	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-8fhc-q55v-jvx2	A flaw was found in Red Hat's AMQ-Streams, which ships a version of the OKHttp component with an information disclosure flaw via an exception triggered by a header containing an illegal value. This issue could allow an authenticated attacker to access information outside of their regular permissions.	2023-09-27	2023-09-27

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 82.86 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2022-44730

Description

Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache XML Graphics Batik. This issue affects Apache XML Graphics Batik: 1.16. A malicious SVG can probe user profile / data and send it directly as parameter to a URL.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-44730

Affected Components

Component	Artifact Id	Version
\${project.groupId}:\${project.artifactId}	batik-script-1.14.jar	1.14

Weakness

CWE-918

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-2474-2566-3qxp	Apache Batik information disclosure vulnerability	2023-08-22	2023-08-22

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.27 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 31.40 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2022-44729

Description

Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache XML Graphics Batik. This issue affects Apache XML Graphics Batik: 1.16. On version 1.16, a malicious SVG could trigger loading external resources by default, causing resource consumption or in some cases even information disclosure. Users are recommended to upgrade to version 1.17 or later.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-44729

Affected Components

Component	Artifact Id	Version
\${project.groupId}:\${project.artifactId}	batik-bridge-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-transcoder-1.14.jar	1.14

Weakness

CWE-918

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-gq5f-xv48-2365	Apache XML Graphics Batik Server-Side Request Forgery vulnerability	2023-08-22	2023-08-22

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.16 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 46.73 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2022-4245

Description

A flaw was found in codehaus-plexus. The org.codehaus.plexus.util.xml.XmlWriterUtil#writeComment fails to sanitize comments for a --> sequence. This issue means that text contained in the command string could be interpreted as XML and allow for XML injection.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-4245

Affected Components

Component	Artifact Id	Version
Plexus Common Utilities	plexus-utils-2.0.6.jar	2.0.6

Weakness

CWE-91, CWE-611

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	4.3	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-jcwr-x25h-x5fh	codehaus-plexus vulnerable to XML injection	2023-09-25	2023-09-25

Assessment

Summary

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

CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi} Page 29 of 290 Doc. Date: \${document.date_

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.34 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 27.76 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2022-4244

Description

A flaw was found in codeplex-codehaus. A directory traversal attack (also known as path traversal) aims to access files and directories stored outside the intended folder. By manipulating files with "dot-dot-slash (../)" sequences and their variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on the file system, including application source code, configuration, and other critical system files.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-4244

Affected Components

Component	Artifact Id	Version
Plexus Common Utilities	plexus-utils-2.0.6.jar	2.0.6

Weakness

CWE-22

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-g6ph-x5wf-g337	plexus-codehaus vulnerable to directory traversal	2023-09-25	2023-09-25

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.11 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 54.03 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2022-41881

Description

Netty project is an event-driven asynchronous network application framework. In versions prior to 4.1.86.Final, a StackOverflowError can be raised when parsing a malformed crafted message due to an infinite recursion. This issue is patched in version 4.1.86.Final. There is no workaround, except using a custom HaProxyMessageDecoder.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-41881

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-674

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-fx2c-96vj-985v	HAProxyMessageDecoder Stack Exhaustion DoS	2022-12-12	2022-12-12

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.19 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 42.74 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2022-34169

Description

The Apache Xalan Java XSLT library is vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode. Users are recommended to update to version 2.7.3 or later. Note: Java runtimes (such as OpenJDK) include repackaged copies of Xalan.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-34169

Affected Components

Component	Artifact Id	Version
	xalan-2.7.2.jar	2.7.2
Xalan Java Serializer	serializer-2.7.2.jar	2.7.2

Weakness

CWE-681

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-9339-86wc-4qgf	Apache Xalan Java XSLT library integer truncation issue when processing malicious XSLT stylesheets	2022-07-20	2022-07-20

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.16 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 45.73 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2022-24823

Doc. Identifier: \${document.id}

Description

Netty is an open-source, asynchronous event-driven network application framework. The package `io.netty:netty-codechttp` prior to version 4.1.77. Final contains an insufficient fix for CVE-2021-21290. When Netty's multipart decoders are used local information disclosure can occur via the local system temporary directory if temporary storing uploads on the disk is enabled. This only impacts applications running on Java version 6 and lower. Additionally, this vulnerability impacts code running on Unix-like systems, and very old versions of Mac OSX and Windows as they all share the system temporary directory between all users. Version 4.1.77. Final contains a patch for this vulnerability. As a workaround, specify one's own 'java.io.tmpdir' when starting the JVM or use DefaultHttpDataFactory.setBaseDir(...) to set the directory to something that is only readable by the current user.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-24823

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-378, CWE-668

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.5	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	1.9	AV:L/AC:M/Au:N/C:P/I:N/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-269q-hmxg-m83q	Local Information Disclosure Vulnerability in io.netty:netty-codec-http	2022-05-10	2022-05-10

Assessment

Summary

Default	Medium
	Default

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 88.26 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.

Criteria	Explanation
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2022-1271

Description

An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-1271

Affected Components

Component	Artifact Id	Version
XZ for Java	xz-1.9.jar	1.9

Weakness

CWE-179, CWE-20

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-jrpw-543v-8r62	An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system.	2022-09-01	2022-09-01

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.24 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 13.98 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2021-43797

Description

Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. Netty prior to version 4.1.71. Final skips control chars when they are present at the beginning / end of the header name. It should instead fail fast as these are not allowed by the spec and could lead to HTTP request smuggling. Failing to do the validation might cause netty to "sanitize" header names before it forward these to another remote system when used as proxy. This remote system can't see the invalid usage anymore, and therefore does not do the validation itself. Users should upgrade to version 4.1.71. Final.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-43797

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-444

Initial Severity

Doc. Identifier: \${document.id}

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-wx5j-54mm-rqqq	HTTP request smuggling in netty	2021-12-09	2021-12-09

Assessment

Summary

Insignificant Default Me

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.40 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 25.61 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-4277

Description

A vulnerability, which was classified as problematic, has been found in fredsmith utils. This issue affects some unknown processing of the file screenshot_sync of the component Filename Handler. The manipulation leads to predictable from observable state. The name of the patch is dbab1b66955eeb3d76b34612b358307f5c4e3944. It is recommended to apply a patch to fix this issue. The identifier VDB-216749 was assigned to this vulnerability.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-4277

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils-0.14.6.jar	0.14.6

Weakness

CWE-341, CWE-330

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:L/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-3cqm-26w8-85g8	A vulnerability, which was classified as problematic, has been found in fredsmith utils. This issue affects some unknown processing of the file screenshot_sync of the component Filename Handler. The manipulation leads to predictable from observable state. The name of the patch is dbab1b66955eeb3d76b34612b358307f5c4e3944. It is recommended to apply a patch to fix this issue. The identifier VDB-216749 was assigned to this vulnerability.	2022-12-25	2022-12-25

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

	o
Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.06 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 72.31 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-37137

Description

The Snappy frame decoder function doesn't restrict the chunk length which may lead to excessive memory usage. Beside this it also may buffer reserved skippable chunks until the whole chunk was received which may lead to excessive memory

usage as well. This vulnerability can be triggered by supplying malicious input that decompresses to a very big size (via a network stream or a file) or by sending a huge skippable chunk.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-37137

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-400

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-9vjp-v76f-g363	SnappyFrameDecoder doesn't restrict chunk length any may buffer skippable chunks in an unnecessary way	2021-09-09	2021-09-09

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.44 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 12.86 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.

Doc. Identifier: \${document.id}

\${document.name} Page 39 of 290 Doc. Version: \${document.versic Doc. Date: \${document.date_

Criteria	Explanation
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2021-37136

Description

The Bzip2 decompression decoder function doesn't allow setting size restrictions on the decompressed output data (which affects the allocation size used during decompression). All users of Bzip2Decoder are affected. The malicious input can trigger an OOME and so a DoS attack

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-37136

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-400

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-grg4-wf29-r9vv	Bzip2Decoder doesn't allow setting size restrictions for decompressed data	2021-09-09	2021-09-09

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.44 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 12.86 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2021-35939

Description

It was found that the fix for CVE-2017-7500 and CVE-2017-7501 was incomplete: the check was only implemented for the parent directory of the file to be created. A local unprivileged user who owns another ancestor directory could potentially use this flaw to gain root privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-35939

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-59

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.7	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-prgv-w33h-5m73	It was found that the fix for CVE-2017-7500 and CVE-2017-7501 was incomplete: the check was only implemented for the parent directory of the file to be created. A local unprivileged user who owns another ancestor directory could potentially use this flaw to gain root privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2022-08-27	2022-08-27

Doc. Identifier: \${document.id} \${document.name} Doc. Version: \${document.versions before the company of the co

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.10 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 58.06 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-35938

Description

A symbolic link issue was found in rpm. It occurs when rpm sets the desired permissions and credentials after installing a file. A local unprivileged user could use this flaw to exchange the original file with a symbolic link to a security-critical file and escalate their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-35938

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-59

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.7	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-83gm-5269-qr3v	A symbolic link issue was found in rpm. It occurs when rpm sets the desired permissions and credentials after installing a file. A local unprivileged user could use this flaw to exchange the original file with a symbolic link to a security-critical file and escalate their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2022-08-26	2022-08-26

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.10 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 58.06 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-35937

Description

A race condition vulnerability was found in rpm. A local unprivileged user could use this flaw to bypass the checks that were introduced in response to CVE-2017-7500 and CVE-2017-7501, potentially gaining root privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-35937

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-59, CWE-367

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.4	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-63x9-9q4w-j636	A race condition vulnerability was found in rpm. A local unprivileged user could use this flaw to bypass the checks that were introduced in response to CVE-2017-7500 and CVE-2017-7501, potentially gaining root privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2022-08-26	2022-08-26

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.10 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 56.53 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-3521

Description

There is a flaw in RPM's signature functionality. OpenPGP subkeys are associated with a primary key via a "binding signature." RPM does not check the binding signature of subkeys prior to importing them. If an attacker is able to add or socially engineer another party to add a malicious subkey to a legitimate public key, RPM could wrongly trust a malicious signature. The greatest impact of this flaw is to data integrity. To exploit this flaw, an attacker must either compromise an RPM repository or convince an administrator to install an untrusted RPM or public key. It is strongly recommended to only use RPMs and public keys from trusted sources.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-3521

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-347

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	4.7	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-pr6x-p264-jrpq	There is a flaw in RPM's signature functionality. OpenPGP subkeys are associated with a primary key via a "binding signature." RPM does not check the binding signature of subkeys prior to importing them. If an attacker is able to add or socially engineer another party to add a malicious subkey to a legitimate public key, RPM could wrongly trust a malicious signature. The greatest impact of this flaw is to data integrity. To exploit this flaw, an attacker must either compromise an RPM repository or convince an administrator to install an untrusted RPM or public key. It is strongly recommended to only use RPMs and public keys from trusted sources.	2022-08-23	2022-08-23

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.07 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 67.63 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-3421

Description

A flaw was found in the RPM package in the read functionality. This flaw allows an attacker who can convince a victim to install a seemingly verifiable package or compromise an RPM repository, to cause RPM database corruption. The highest threat from this vulnerability is to data integrity. This flaw affects RPM versions before 4.17.0-alpha.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-3421

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-347

Initial Severity

Doc. Identifier: \${document.id}

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.5	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-f7ww-c7v4-g682	A flaw was found in the RPM package in the read functionality. This flaw allows an attacker who can convince a victim to install a seemingly verifiable package or compromise an RPM repository, to cause RPM database corruption. The highest threat from this vulnerability is to data integrity. This flaw affects RPM versions before 4.17.0-alpha.	2022-05-24	2022-05-24

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

	' ,
Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.07 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 67.53 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-33813

Description

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

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-33813

Affected Components

Component	Artifact Id	Version
JDOM	jdom2-2.0.6.1.jar	2.0.6.1

Weakness

CWE-611

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-2363-cqg2-863c	XML External Entity (XXE) Injection in JDOM	2021-07-27	2021-07-27

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.48 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 23.42 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2021-26291

Description

Apache Maven will follow repositories that are defined in a dependency's Project Object Model (pom) which may be surprising to some users, resulting in potential risk if a malicious actor takes over that repository or is able to insert themselves into a position to pretend to be that repository. Maven is changing the default behavior in 3.8.1+ to no longer follow http (non-SSL) repository references by default. More details available in the referenced urls. If you are currently using a repository manager to govern the repositories used by your builds, you are unaffected by the risks present in the legacy behavior,

and are unaffected by this vulnerability and change to default behavior. See this link for more information about repository management: https://maven.apache.org/repository-management.html

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-26291

Affected Components

Component	Artifact Id	Version
Apache Maven Reporting Implementation	maven-reporting-impl-3.2.0.jar	3.2.0
Maven Model	maven-model-3.0.5.jar	3.0.5
Maven Core	maven-core-3.0.5.jar	3.0.5
Doxia :: Logging API	doxia-logging-api-1.11.1.jar	1.11.1
Maven Plugin Tools Extractor API	maven-plugin-tools-api-3.7.0.jar	3.7.0
Maven Plugin Tool for Java with Javadoc Tags	maven-plugin-tools-java-3.7.0.jar	3.7.0
Maven Settings Builder	maven-settings-builder-3.0.5.jar	3.0.5
Maven Aether Provider	maven-aether-provider-3.0.5.jar	3.0.5
Apache Maven Reporting API	maven-reporting-api-3.1.1.jar	3.1.1
Maven Plugin Plugin	maven-plugin-3.7.0.jar	3.7.0
Maven Plugin Tools Java 5 Annotations	maven-plugin-annotations-3.5.jar	3.5
Maven Artifact	maven-artifact-3.0.5.jar	3.0.5
Doxia Sitetools :: Integration Tools	doxia-integration-tools-1.11.1.jar	1.11.1
Doxia :: XHTML5 Module	doxia-module-xhtml5-1.11.1.jar	1.11.1
Maven Plugin Tool for Java with Annotations	maven-plugin-tools-annotations-3.7.0.jar	3.7.0
Doxia :: Sink API	doxia-sink-api-1.11.1.jar	1.11.1
Apache Maven Wagon :: API	wagon-provider-api-2.4.jar	2.4
Maven Repository Metadata Model	maven-repository-metadata-3.0.5.jar	3.0.5
Doxia :: Core	doxia-core-1.11.1.jar	1.11.1
Maven Plugin Tools Generators	maven-plugin-tools-generators-3.7.0.jar	3.7.0
Maven Model Builder	maven-model-builder-3.0.5.jar	3.0.5
Doxia :: XHTML Module	doxia-module-xhtml-1.11.1.jar	1.11.1
Maven Settings	maven-settings-3.0.5.jar	3.0.5
Doxia Sitetools :: Skin Model	doxia-skin-model-1.11.1.jar	1.11.1
Maven Plugin API	maven-plugin-api-3.0.5.jar	3.0.5
Maven Compat	maven-compat-3.0.5.jar	3.0.5
Doxia Sitetools :: Site Renderer	doxia-site-renderer-1.11.1.jar	1.11.1
Doxia Sitetools :: Decoration Model	doxia-decoration-model-1.11.1.jar	1.11.1

Weakness

CWE-346

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:H/A:N	Critical
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-2f88-5hg8-9x2x	Origin Validation Error in Apache Maven	2021-06-16	2021-06-16

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.20 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 41.61 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2021-25738

Description

Loading specially-crafted yaml with the Kubernetes Java Client library can lead to code execution.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-25738

Affected Components

Component	Artifact Id	Version
Fabric8 :: Kubernetes :: Java Client API	kubernetes-client-api-6.13.3.jar	6.13.3

Weakness

CWE-20, CWE-502

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.7	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	Medium
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-m8wh-mqgf-rr8g	Code injection in Kubernetes Java Client	2021-10-12	2021-10-12

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 82.63 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-24028

Description

An invalid free in Thrift's table-based serialization can cause the application to crash or potentially result in code execution or other undesirable effects. This issue affects Facebook Thrift prior to v2021.02.22.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-24028

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-763

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-qrr3-c36x-2pcc	An invalid free in Thrift's table-based serialization can cause the application to crash or potentially result in code execution or other undesirable effects. This issue affects Facebook Thrift prior to v2021.02.22.00.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.36 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 27.12 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2021-21409

Description

Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty (io.netty:netty-codec-http2) before version 4.1.61.Final there is a vulnerability that enables request smuggling. The content-length header is not correctly validated if the request only uses a single Http2HeaderFrame with the endStream set to to true. This could lead to request smuggling if the request is proxied to a remote peer and translated to HTTP/1.1. This is a followup of GHSA-wm47-8v5p-wjpj/CVE-2021-21295 which did miss to fix this one case. This was fixed as part of 4.1.61.Final.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-21409

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-444

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:H/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-f256-j965-7f32	Possible request smuggling in HTTP/2 due missing validation of content-length	2021-03-30	2021-03-30

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.80 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 11.40 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-21295

Description

Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty (io.netty:netty-codec-http2) before version 4.1.60. Final there is a vulnerability that enables request smuggling. If a Content-Length header is present in the original HTTP/2 request, the field is not validated by `Http2MultiplexHandler` as it is propagated up. This is fine as long as the request is not proxied through as HTTP/1.1. If the request comes in as an HTTP/2 stream, gets converted into the HTTP/1.1 domain objects (`HttpRequest`, `HttpContent`, etc.) via `Http2StreamFrameToHttpObjectCodec `and then sent up to the child channel's pipeline and proxied through a remote peer as HTTP/1.1 this may result in request smuggling. In a proxy case, users may assume the content-length is validated somehow, which is not the case. If the request is forwarded to a backend channel that is a HTTP/1.1 connection, the Content-Length now has meaning and needs to be checked. An attacker can smuggle requests inside the body as it gets downgraded from HTTP/2 to HTTP/1.1. For an example attack refer to the linked GitHub Advisory. Users are only affected if all of this is true: `HTTP2MultiplexCodec` or `Http2FrameCodec` is used, `Http2StreamFrameToHttpObjectCodec` is used to convert to HTTP/1.1 objects, and these HTTP/1.1 objects are forwarded to another remote peer. This has been patched in 4.1.60.Final As a workaround, the user can do the validation by themselves by implementing a custom `ChannelInboundHandler` that is put in the `ChannelPipeline` behind `Http2StreamFrameToHttpObjectCodec`.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-21295

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-444

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:H/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-wm47-8v5p-wjpj	Possible request smuggling in HTTP/2 due missing validation	2021-03-09	2021-03-09

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Doc. Identifier: \${document.id}

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 16.21 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 3.86 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-21290

Description

Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty before version 4.1.59. Final there is a vulnerability on Unix-like systems involving an insecure temp file. When netty's multipart decoders are used local information disclosure can occur via the local system temporary directory if temporary storing uploads on the disk is enabled. On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissions can lead to information disclosure. Of note, this does not impact modern MacOS Operating Systems. The method "File.createTempFile" on unix-like systems creates a random file, but, by default will create this file with the permissions "-rw-r--r--". Thus, if sensitive information is written to this file, other local users can read this information. This is the case in netty's "AbstractDiskHttpData" is vulnerable. This has been fixed in version 4.1.59. Final. As a workaround, one may specify your own "java.io.tmpdir" when you start the JVM or use "DefaultHttpDataFactory.setBaseDir(...)" to set the directory to something that is only readable by the current user.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-21290

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-378, CWE-668

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.5	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	1.9	AV:L/AC:M/Au:N/C:P/I:N/A:N	Low

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-5mcr-gq6c-3hq2	Local Information Disclosure Vulnerability in Netty on Unix-Like systems	2021-02-08	2021-02-08

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi} Page 56 of 290 Doc. Date: \${document.date_

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 85.15 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-20266

Description

A flaw was found in RPM's hdrblobInit() in lib/header.c. This flaw allows an attacker who can modify the rpmdb to cause an out-of-bounds read. The highest threat from this vulnerability is to system availability.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-20266

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-125

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	4.9	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H	Medium
CVSS:2.0	NVD-CNA-NVD	4.0	AV:N/AC:L/Au:S/C:N/I:N/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-8vf3-43pf-v3cq	A flaw was found in RPM's hdrbloblnit() in lib/header.c. This flaw allows an attacker who can modify the rpmdb to cause an out-of-bounds read. The highest threat from this vulnerability is to system availability.	2022-05-24	2022-05-24

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.17 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 44.45 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2020-8908

Description

A temp directory creation vulnerability exists in all versions of Guava, allowing an attacker with access to the machine to potentially access data in a temporary directory created by the Guava API com.google.common.io.Files.createTempDir(). By default, on unix-like systems, the created directory is world-readable (readable by an attacker with access to the system). The method in question has been marked @Deprecated in versions 30.0 and later and should not be used. For Android developers, we recommend choosing a temporary directory API provided by Android, such as context.getCacheDir(). For other Java developers, we recommend migrating to the Java 7 API java.nio.file.Files.createTempDirectory() which explicitly configures permissions of 700, or configuring the Java runtime's java.io.tmpdir system property to point to a location whose permissions are appropriately configured.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-8908

Affected Components

Component	Artifact Id	Version
Guava InternalFutureFailureAccess and InternalFutures	failureaccess-1.0.2.jar	1.0.2

Weakness

CWE-378, CWE-732

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi}
Page 58 of 290 Doc. Date: \${document.date_

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	3.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	Low
CVSS:2.0	NVD-CNA-NVD	2.1	AV:L/AC:L/Au:N/C:P/I:N/A:N	Low

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-5mg8-w23w-74h3	Information Disclosure in Guava	2021-03-25	2021-03-25

Assessment

Summary



CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.06 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 72.98 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2020-8570

Doc. Identifier: \${document.id}

Description

Kubernetes Java client libraries in version 10.0.0 and versions prior to 9.0.1 allow writes to paths outside of the current directory when copying multiple files from a remote pod which sends a maliciously crafted archive. This can potentially overwrite any files on the system of the process executing the client code.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-8570

Affected Components

Component	Artifact Id	Version
Fabric8 :: Kubernetes :: Java Client API	kubernetes-client-api-6.13.3.jar	6.13.3

Weakness

CWE-23, CWE-22

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:N/I:H/A:H	Critical
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:N/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-cghx-9gcr-r42x	Path Traversal in the Java Kubernetes Client	2021-01-29	2021-01-29

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.43 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 24.95 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2020-8554

Description

Kubernetes API server in all versions allow an attacker who is able to create a ClusterIP service and set the spec.externalIPs field, to intercept traffic to that IP address. Additionally, an attacker who is able to patch the status (which is considered a privileged operation and should not typically be granted to users) of a LoadBalancer service can set the status.loadBalancer.ingress.ip to similar effect.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-8554

Affected Components

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Apps	kubernetes-model-apps-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Metrics	kubernetes-model-metrics-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Autoscaling	kubernetes-model-autoscaling-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Storage Class	kubernetes-model-storageclass-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: API Extensions	kubernetes-model-apiextensions-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Networking	kubernetes-model-networking-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Scheduling	kubernetes-model-scheduling-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes :: HttpClient :: OkHttp	kubernetes-httpclient-okhttp-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Common	kubernetes-model-common-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Policy	kubernetes-model-policy-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Discovery	kubernetes-model-discovery-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Core	kubernetes-model-core-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Sigs :: Gateway API	kubernetes-model-gatewayapi-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Batch	kubernetes-model-batch-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: RBAC	kubernetes-model-rbac-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Resource	kubernetes-model-resource-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Certificates	kubernetes-model-certificates-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Node	kubernetes-model-node-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: FlowControl	kubernetes-model-flowcontrol-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Coordination	kubernetes-model-coordination-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Extensions	kubernetes-model-extensions-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes :: Java Client API	kubernetes-client-api-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Admission Registration, Authentication and Authorization	kubernetes-model-admissionregistration-6.13.3.jar	6.13.3
Fabric8 :: Kubernetes Model :: Events	kubernetes-model-events-6.13.3.jar	6.13.3

Weakness

CWE-283

Doc. Identifier: \${document.id} \${document.name} Doc. Version: \${document.versions before the company of the co

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.0	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L	Medium
CVSS:2.0	NVD-CNA-NVD	6.0	AV:N/AC:M/Au:S/C:P/I:P/A:P	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-j9wf-vvm6-4r9w	Unverified Ownership in Kubernetes	2022-02-08	2022-02-08

Assessment

Summary

Insignificant	Default	Medium
•		

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.24 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 37.41 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2020-7768

Description

The package grpc before 1.24.4; the package @grpc/grpc-js before 1.1.8 are vulnerable to Prototype Pollution via loadPackageDefinition.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-7768

Affected Components

Component	Artifact Id	Version
	ae-artifact-flow-grpc-0.135.0.jar	0.135.0

Weakness

CWE-1321

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	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-pp75-xfpw-37g9	Prototype pollution in grpc and @grpc/grpc-js	2021-04-19	2021-04-19

Assessment

Summary



CVSS Vector Severity Charts

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.53 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 22.21 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2020-13959

Description

The default error page for VelocityView in Apache Velocity Tools prior to 3.1 reflects back the vm file that was entered as part of the URL. An attacker can set an XSS payload file as this vm file in the URL which results in this payload being executed. XSS vulnerabilities allow attackers to execute arbitrary JavaScript in the context of the attacked website and the attacked user. This can be abused to steal session cookies, perform requests in the name of the victim or for phishing attacks.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-13959

Affected Components

Component	Artifact Id	Version
VelocityTools	velocity-tools-2.0.jar	2.0

Weakness

CWE-79

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-fh63-4r66-jc7v	Cross-site scripting (XSS) in Apache Velocity Tools	2021-03-12	2021-03-12

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Doc. Identifier: \${document.id}

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.74 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 18.51 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2020-13936

Description

An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-13936

Affected Components

Component	Artifact Id	Version
	velocity-1.7.jar	1.7

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	9.0	AV:N/AC:L/Au:S/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-59j4-wjwp-mw9m	Sandbox Bypass in Apache Velocity Engine	2022-01-06	2022-01-06

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.17 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 44.92 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2020-10683

Description

dom4j before 2.0.3 and 2.1.x before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation from OWASP showing how to enable the safe, non-default behavior in any application that uses dom4j.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-10683

Affected Components

Component	Artifact Id	Version
	dom4j-1.6.1.jar	1.6.1

Weakness

CWE-611

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-hwj3-m3p6-hj38	dom4j allows External Entities by default which might enable XXE attacks	2020-06-05	2020-06-05

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.66 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 19.90 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2020-10519

Description

A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22.7 and was fixed in 2.22.7, 2.21.15, and 2.20.24. The underlying issues contributing to this vulnerability were identified through the GitHub Security Bug Bounty program.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-10519

Affected Components

Component	Artifact Id	Version
jackson-coreutils	jackson-coreutils-2.0.jar	2.0
JSONLD Java :: Core	jsonld-java-0.13.4.jar	0.13.4
json-schema-core	json-schema-core-1.2.14.jar	1.2.14
msg-simple	msg-simple-1.2.jar	1.2
btf	btf-1.3.jar	1.3
juniversalchardet	juniversalchardet-2.4.0.jar	2.4.0

Doc. Identifier: \${document.id} \${document.name} Doc. Page 67 of 290

Component	Artifact Id	Version
uri-template	uri-template-0.10.jar	0.10
jackson-coreutils-equivalence	jackson-coreutils-equivalence-1.0.jar	1.0
curvesapi	curvesapi-1.08.jar	1.08
json-schema-validator	json-schema-validator-2.2.14.jar	2.2.14
zstd-jni	zstd-jni-1.5.2-4.jar	1.5.2-4
Package URL	packageurl-java-1.5.0.jar	1.5.0

Weakness

CWE-77

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-gcp3-gfr7-rcqp	A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. Usercontrolled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22.7 and was fixed in 2.22.7, 2.21.15, and 2.20.24. The underlying issues contributing to this vulnerability were identified through the GitHub Security Bug Bounty program.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versions}Page 68 of 290Doc. Date: \${document.date_

Criteria	Explanation
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.71 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 18.99 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2020-10518

Description

A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in 2.21.6, 2.20.15, and 2.19.21. The underlying issues contributing to this vulnerability were identified both internally and through the GitHub Security Bug Bounty program.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-10518

Affected Components

Component	Artifact Id	Version
jackson-coreutils	jackson-coreutils-2.0.jar	2.0
JSONLD Java :: Core	jsonld-java-0.13.4.jar	0.13.4
json-schema-core	json-schema-core-1.2.14.jar	1.2.14
msg-simple	msg-simple-1.2.jar	1.2
btf	btf-1.3.jar	1.3
juniversalchardet	juniversalchardet-2.4.0.jar	2.4.0
uri-template	uri-template-0.10.jar	0.10
jackson-coreutils-equivalence	jackson-coreutils-equivalence-1.0.jar	1.0
curvesapi	curvesapi-1.08.jar	1.08
json-schema-validator	json-schema-validator-2.2.14.jar	2.2.14
zstd-jni	zstd-jni-1.5.2-4.jar	1.5.2-4
Package URL	packageurl-java-1.5.0.jar	1.5.0

Weakness

Doc. Identifier: \${document.id}

CWE-77

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-m5vm-44r4-56mf	A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. User-controlled configuration of the underlying parsers used by GitHub Pages were not sufficiently restricted and made it possible to execute commands on the GitHub Enterprise Server instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in 2.21.6, 2.20.15, and 2.19.21. The underlying issues contributing to this vulnerability were identified both internally and through the GitHub Security Bug Bounty program.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.29 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 30.35 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2020-10517

Description

An improper access control vulnerability was identified in GitHub Enterprise Server that allowed authenticated users of the instance to determine the names of unauthorized private repositories given their numerical IDs. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in versions 2.21.6, 2.20.15, and 2.19.21. This vulnerability was reported via the GitHub Bug Bounty program.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-10517

Affected Components

Component	Artifact Id	Version
jackson-coreutils	jackson-coreutils-2.0.jar	2.0
JSONLD Java :: Core	jsonld-java-0.13.4.jar	0.13.4
json-schema-core	json-schema-core-1.2.14.jar	1.2.14
msg-simple	msg-simple-1.2.jar	1.2
btf	btf-1.3.jar	1.3
juniversalchardet	juniversalchardet-2.4.0.jar	2.4.0
uri-template	uri-template-0.10.jar	0.10
jackson-coreutils-equivalence	jackson-coreutils-equivalence-1.0.jar	1.0
curvesapi	curvesapi-1.08.jar	1.08
json-schema-validator	json-schema-validator-2.2.14.jar	2.2.14
zstd-jni	zstd-jni-1.5.2-4.jar	1.5.2-4
Package URL	packageurl-java-1.5.0.jar	1.5.0

Weakness

CWE-285

Initial Severity

Doc. Identifier: \${document.id}

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	4.3	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-38rx-7wc7-6jvw	An improper access control vulnerability was identified in GitHub Enterprise Server that allowed authenticated users of the instance to determine the names of unauthorized private repositories given their numerical IDs. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.22 and was fixed in versions 2.21.6, 2.20.15, and 2.19.21. This vulnerability was reported via the GitHub Bug Bounty program.	2022-05-24	2022-05-24

Assessment

Summary

Insignificant	Default	Medium
Insignificant	Detault	wealum

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.06 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 71.03 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2019-3565

Description

Legacy C++ Facebook Thrift servers (using cpp instead of cpp2) would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.05.06.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-3565

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-834, CWE-755

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-j98f-h9mx-xrxq	Legacy C++ Facebook Thrift servers (using cpp instead of cpp2) would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.05.06.00.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.75 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 18.44 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-3564

Description

Go Facebook Thrift servers would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.03.04.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-3564

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-834, CWE-755

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-x4rg-4545-4w7w	Improper Input Validation and Excessive Iteration in Go Facebook Thrift	2021-11-03	2021-11-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

Doc. Identifier: \${document.id}

\${document.name} Page 74 of 290 Doc. Version: \${document.versic Doc. Date: \${document.date_

Criteria	Explanation
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.31 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 29.43 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-3559

Description

Java Facebook Thrift servers would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.02.18.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-3559

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-834, CWE-755

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

Advisories

Doc. Identifier: \${document.id}

Alerts

Id	Summary	Create Date	Update Date
GHSA-6627-jcx5-j2g8	Java Facebook Thrift servers would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.02.18.00.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.31 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 29.43 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-3558

Description

Python Facebook Thrift servers would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.02.18.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-3558

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-834, CWE-755

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

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-7vv7-v9gp-whmr	Python Facebook Thrift servers would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.02.18.00.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.39 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 26.09 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-3553

Description

C++ Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2020.02.03.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-3553

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-770

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-859v-9mcv-7rw3	C++ Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2020.02.03.00.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.19 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 42.50 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-3552

Description

C++ Facebook Thrift servers (using cpp2) would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.02.18.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-3552

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-834, CWE-755

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-h27g-g76x-xqpw	C++ Facebook Thrift servers (using cpp2) would not error upon receiving messages with containers of fields of unknown type. As a result, malicious clients could send short messages which would take a long time for the server to parse, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.02.18.00.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.24 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 37.27 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-20445

Description

HttpObjectDecoder.java in Netty before 4.1.44 allows a Content-Length header to be accompanied by a second Content-Length header, or by a Transfer-Encoding header.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-20445

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-444

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:H/A:N	Critical
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-p2v9-g2qv-p635	HTTP Request Smuggling in Netty	2020-02-21	2020-02-21

Assessment

Summary



Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versions}Page 80 of 290Doc. Date: \${document.date_

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.18 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 43.91 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-20444

Description

HttpObjectDecoder.java in Netty before 4.1.44 allows an HTTP header that lacks a colon, which might be interpreted as a separate header with an incorrect syntax, or might be interpreted as an "invalid fold."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-20444

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-444

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:H/A:N	Critical
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-cqqj-4p63-rrmm	HTTP Request Smuggling in Netty	2020-02-21	2020-02-21

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

	·
Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.86 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 17.05 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-16869

Description

Netty before 4.1.42. Final mishandles whitespace before the colon in HTTP headers (such as a "Transfer-Encoding : chunked" line), which leads to HTTP request smuggling.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-16869

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-444

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-p979-4mfw-53vg	HTTP Request Smuggling in Netty	2019-10-11	2019-10-11

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.22 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 10.12 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-11939

Description

Golang Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2020.03.16.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-11939

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-770

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-w3r9-r9w7-8h48	Golang Facebook Thrift servers vulnerable to denial of service	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.12 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 53.07 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-11938

Description

Java Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.12.09.00.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-11938

Affected Components

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Weakness

CWE-770

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-hr4p-8hm2-w85x	Java Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.12.09.00.	2022-05-24	2022-05-24

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.19 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 42.50 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2019-10086

Description

In Apache Commons Beanutils 1.9.2, a special BeanIntrospector class was added which allows suppressing the ability for an attacker to access the classloader via the class property available on all Java objects. We, however were not using this by default characteristic of the PropertyUtilsBean.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-10086

Affected Components

Component	Artifact Id	Version
	commons-beanutils-1.7.0.jar	1.7.0

Weakness

CWE-502

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-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-6phf-73q6-gh87	Insecure Deserialization in Apache Commons Beanutils	2020-06-15	2020-06-15

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.39 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 25.84 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2018-6969

Description

VMware Tools (10.x and prior before 10.3.0) contains an out-of-bounds read vulnerability in HGFS. Successful exploitation of this issue may lead to information disclosure or may allow attackers to escalate their privileges on the guest VMs. In order to be able to exploit this issue, file sharing must be enabled.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-6969

Affected Components

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

Weakness

CWE-125

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.0	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	High
CVSS:2.0	NVD-CNA-NVD	4.4	AV:L/AC:M/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-qc3q-9h28-r994	VMware Tools (10.x and prior before 10.3.0) contains an out-of-bounds read vulnerability in HGFS. Successful exploitation of this issue may lead to information disclosure or may allow attackers to escalate their privileges on the guest VMs. In order to be able to exploit this issue, file sharing must be enabled.	2022-05-14	2022-05-14

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.05 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 77.73 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2018-1000632

Description

dom4j version prior to version 2.1.1 contains a CWE-91: XML Injection vulnerability in Class: Element. Methods: addElement, addAttribute that can result in an attacker tampering with XML documents through XML injection. This attack appear to be exploitable via an attacker specifying attributes or elements in the XML document. This vulnerability appears to have been fixed in 2.1.1 or later.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1000632

Affected Components

Component	Artifact Id	Version
	dom4j-1.6.1.jar	1.6.1

Weakness

CWE-91

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-6pcc-3rfx-4gpm	Dom4j contains a XML Injection vulnerability	2018-10-16	2018-10-16

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.37 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 26.78 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2017-9530

Description

IrfanView version 4.44 (32bit) might allow attackers to cause a denial of service or execute arbitrary code via a crafted file, related to "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at ntdll_77df0000!LdrpResCompareResourceNames+0x0000000000000150."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2017-9530

Affected Components

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

Weakness

CWE-119

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	High
CVSS:2.0	NVD-CNA-NVD	4.4	AV:L/AC:M/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-cx97-5qm7-6wq7	IrfanView version 4.44 (32bit) might allow attackers to cause a denial of service or execute arbitrary code via a crafted file, related to "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at ntdll_77df0000! LdrpResCompareResourceNames+0x000000000000150."	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.13 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 50.51 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2017-9431

Description

Google gRPC before 2017-04-05 has an out-of-bounds write caused by a heap-based buffer overflow related to core/lib/iomgr/error.c.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2017-9431

Affected Components

Component	Artifact Id	Version
	ae-artifact-flow-grpc-0.135.0.jar	0.135.0

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
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-6q3h-fg8c-jqrj	Google gRPC before 2017-04-05 has an out-of-bounds write caused by a heap-based buffer overflow related to core/lib/iomgr/error.c.	2022-05-17	2022-05-17

Assessment

Summary



Doc. Version: \${document.version: Doc. Date: \${document.date_

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.25 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 33.95 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2017-8359

Description

Google gRPC before 2017-03-29 has an out-of-bounds write caused by a heap-based use-after-free related to the grpc_call_destroy function in core/lib/surface/call.c.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2017-8359

Affected Components

Component	Artifact Id	Version
	ae-artifact-flow-grpc-0.135.0.jar	0.135.0

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
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-j2fw-rfr9-pfrh	Google gRPC before 2017-03-29 has an out-of-bounds write caused by a heap-based use-after-free related to the grpc_call_destroy function in core/lib/surface/call.c.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.75 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 18.41 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2017-7861

Description

Google gRPC before 2017-02-22 has an out-of-bounds write related to the gpr_free function in core/lib/support/alloc.c.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2017-7861

Affected Components

Component	Artifact Id	Version
	ae-artifact-flow-grpc-0.135.0.jar	0.135.0

Weakness

CWE-787

Doc. Identifier: \${document.id} \${document.name} Doc. Version: \${document.versions before the company of the co

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-wgxc-2fq5-r7v3	Google gRPC before 2017-02-22 has an out-of-bounds write related to the gpr_free function in core/lib/support/alloc.c.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.63 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 20.28 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2017-7860

Description

Google gRPC before 2017-02-22 has an out-of-bounds write caused by a heap-based buffer overflow related to the parse_unix function in core/ext/client_channel/parse_address.c.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2017-7860

Affected Components

Component	Artifact Id	Version
	ae-artifact-flow-grpc-0.135.0.jar	0.135.0

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
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-j8v6-6xq3-6m4f	Google gRPC before 2017-02-22 has an out-of-bounds write caused by a heap-based buffer overflow related to the parse_unix function in core/ext/client_channel/parse_address.c.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.58 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 21.21 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2017-7501

Description

It was found that versions of rpm before 4.13.0.2 use temporary files with predictable names when installing an RPM. An attacker with ability to write in a directory where files will be installed could create symbolic links to an arbitrary location and modify content, and possibly permissions to arbitrary files, which could be used for denial of service or possibly privilege escalation.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2017-7501

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-59

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
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-3xgr-x5gv-64gh	It was found that versions of rpm before 4.13.0.2 use temporary files with predictable names when installing an RPM. An attacker with ability to write in a directory where files will be installed could create symbolic links to an arbitrary location and modify content, and possibly permissions to arbitrary files, which could be used for denial of service or possibly privilege escalation.	2022-05-13	2022-05-13

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.06 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 73.41 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2017-1000487

Description

Plexus-utils before 3.0.16 is vulnerable to command injection because it does not correctly process the contents of double quoted strings.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2017-1000487

Affected Components

Component	Artifact Id	Version
Plexus Common Utilities	plexus-utils-2.0.6.jar	2.0.6

Weakness

CWE-78

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

Advisories

Doc. Identifier: \${document.id}

Alerts

ld	Summary	Create Date	Update Date
GHSA-8vhq-qq4p-grq3	OS Command Injection in Plexus-utils	2022-05-13	2022-05-13

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.39 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 25.82 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2016-7080

Description

The graphic acceleration functions in VMware Tools 9.x and 10.x before 10.0.9 on OS X allow local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors, a different vulnerability than CVE-2016-7079.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2016-7080

Affected Components

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

Weakness

CWE-476

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
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-cp2g-849g-w9jr	The graphic acceleration functions in VMware Tools 9.x and 10.x before 10.0.9 on OS X allow local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors, a different vulnerability than CVE-2016-7079.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2016-7079

Description

The graphic acceleration functions in VMware Tools 9.x and 10.x before 10.0.9 on OS X allow local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors, a different vulnerability than CVE-2016-7080.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2016-7079

Affected Components

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

Weakness

CWE-476

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
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-wxpj-3x4g-grwp	The graphic acceleration functions in VMware Tools 9.x and 10.x before 10.0.9 on OS X allow local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors, a different vulnerability than CVE-2016-7080.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2016-5328

Doc. Identifier: \${document.id}

Description

VMware Tools 9.x and 10.x before 10.1.0 on OS X, when System Integrity Protection (SIP) is enabled, allows local users to determine kernel memory addresses and bypass the kASLR protection mechanism via unspecified vectors.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2016-5328

Affected Components

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

Weakness

CWE-200

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.5	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	2.1	AV:L/AC:L/Au:N/C:P/I:N/A:N	Low

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-4h47-vq45-ccw2	VMware Tools 9.x and 10.x before 10.1.0 on OS X, when System Integrity Protection (SIP) is enabled, allows local users to determine kernel memory addresses and bypass the kASLR protection mechanism via unspecified vectors.	2022-05-17	2022-05-17

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.

Doc. Identifier: \${document.id}

\${document.name} Page 101 of 290 Doc. Version: \${document.version: Doc. Date: \${document.date_

Criteria	Explanation
Assessment	The vulnerability status is insignificant .

CVE-2015-5191

Description

VMware Tools prior to 10.0.9 contains multiple file system races in libDeployPkg, related to the use of hard-coded paths under /tmp. Successful exploitation of this issue may result in a local privilege escalation. CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2015-5191

Affected Components

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

Weakness

CWE-362

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.7	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Medium
CVSS:2.0	NVD-CNA-NVD	3.7	AV:L/AC:H/Au:N/C:P/I:P/A:P	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-4vr2-36wr-v82r	VMware Tools prior to 10.0.9 contains multiple file system races in libDeployPkg, related to the use of hard-coded paths under /tmp. Successful exploitation of this issue may result in a local privilege escalation. CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	2022-05-17	2022-05-17

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

\${product.watermark.name}

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2015-4035

Description

scripts/xzgrep.in in xzgrep 5.2.x before 5.2.0, before 5.0.0 does not properly process file names containing semicolons, which allows remote attackers to execute arbitrary code by having a user run xzgrep on a crafted file name.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2015-4035

Affected Components

Component	Artifact Id	Version
XZ for Java	xz-1.9.jar	1.9

Weakness

CWE-20

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
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-mf33-8p24-6h53	scripts/xzgrep.in in xzgrep 5.2.x before 5.2.0, before 5.0.0 does not properly process file names containing semicolons, which allows remote attackers to execute arbitrary code by having a user run xzgrep on a crafted file name.	2022-05-14	2022-05-14

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.41 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 25.52 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2015-2156

Description

Netty before 3.9.8.Final, 3.10.x before 3.10.3.Final, 4.0.x before 4.0.28.Final, and 4.1.x before 4.1.0.Beta5 and Play Framework 2.x before 2.3.9 might allow remote attackers to bypass the httpOnly flag on cookies and obtain sensitive information by leveraging improper validation of cookie name and value characters.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2015-2156

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-20

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

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-xfv3-rrfm-f2rv	Information Exposure in Netty	2020-06-30	2020-06-30

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.56 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 21.65 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2014-8118

Description

Integer overflow in RPM 4.12 and earlier allows remote attackers to execute arbitrary code via a crafted CPIO header in the payload section of an RPM file, which triggers a stack-based buffer overflow.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2014-8118

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-189

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-wj3v-j872-6xqx	Integer overflow in RPM 4.12 and earlier allows remote attackers to execute arbitrary code via a crafted CPIO header in the payload section of an RPM file, which triggers a stack-based buffer overflow.	2022-05-14	2022-05-14

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 36.79 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 2.71 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2014-4200

Description

vm-support 0.88 in VMware Tools, as distributed with VMware Workstation through 10.0.3 and other products, uses 0644 permissions for the vm-support archive, which allows local users to obtain sensitive information by extracting files from this archive.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2014-4200

Affected Components

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

Weakness

CWE-264

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.7	AV:L/AC:M/Au:N/C:C/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-959q-xwwj-g697	vm-support 0.88 in VMware Tools, as distributed with VMware Workstation through 10.0.3 and other products, uses 0644 permissions for the vm-support archive, which allows local users to obtain sensitive information by extracting files from this archive.	2022-05-17	2022-05-17

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:M/Au:N/C:C/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2014-4199

Description

vm-support 0.88 in VMware Tools, as distributed with VMware Workstation through 10.0.3 and other products, allows local users to write to arbitrary files via a symlink attack on a file in /tmp.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2014-4199

Affected Components

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

Weakness

CWE-59

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.3	AV:L/AC:M/Au:N/C:N/I:C/A:C	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-v55p-68fc-xxcv	vm-support 0.88 in VMware Tools, as distributed with VMware Workstation through 10.0.3 and other products, allows local users to write to arbitrary files via a symlink attack on a file in /tmp.	2022-05-17	2022-05-17

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:M/Au:N/C:N/I:C/A:C
Keywords	No keyword sets matched.

Doc. Identifier: \${document.id}

\${document.name} Page 108 of 290 Doc. Version: \${document.versic Doc. Date: \${document.date_

Criteria	Explanation
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2014-3488

Description

The SslHandler in Netty before 3.9.2 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted SSLv2Hello message.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2014-3488

Affected Components

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

Weakness

CWE-119

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-9959-6p3m-wxpc	Denial of service in Netty	2020-06-30	2020-06-30

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.12 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 14.84 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2014-0114

Description

Apache Commons BeanUtils, as distributed in lib/commons-beanutils-1.8.0.jar in Apache Struts 1.x through 1.3.10 and in other products requiring commons-beanutils through 1.9.2, does not suppress the class property, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via the class parameter, as demonstrated by the passing of this parameter to the getClass method of the ActionForm object in Struts 1.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2014-0114

Affected Components

Component	Artifact Id	Version
	commons-beanutils-1.7.0.jar	1.7.0

Weakness

CWE-20

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Doc. Identifier: \${document.id}

Alerts

Id	Summary	Create Date	Update Date
GHSA-p66x-2cv9-qq3v	Arbitrary code execution in Apache Commons BeanUtils	2020-06-10	2020-06-10

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

(9.4 from base score 7.5)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 97.27 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 0.11 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2013-6435

Description

Race condition in RPM 4.11.1 and earlier allows remote attackers to execute arbitrary code via a crafted RPM file whose installation extracts the contents to temporary files before validating the signature, as demonstrated by installing a file in the /etc/cron.d directory.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2013-6435

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-74

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.6	AV:N/AC:H/Au:N/C:C/I:C/A:C	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-qww5-w98g-66q7	Race condition in RPM 4.11.1 and earlier allows remote attackers to execute arbitrary code via a crafted RPM file whose installation extracts the contents to temporary files before validating the signature, as demonstrated by installing a file in the /etc/cron.d directory.	2022-05-14	2022-05-14

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

	•
Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 9.12 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 5.12 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2012-2055

Description

GitHub Enterprise before 20120304 does not properly restrict the use of a hash to provide values for a model's attributes, which allows remote attackers to set the public_key[user_id] value via a modified URL for the public-key update form, related to a "mass assignment" vulnerability.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2012-2055

Affected Components

Component	Artifact Id	Version
jackson-coreutils	jackson-coreutils-2.0.jar	2.0

Component	Artifact Id	Version
Caffeine cache	caffeine-3.1.8.jar	3.1.8
juniversalchardet	juniversalchardet-2.4.0.jar	2.4.0
jackson-coreutils-equivalence	jackson-coreutils-equivalence-1.0.jar	1.0
json-schema-validator	json-schema-validator-2.2.14.jar	2.2.14
PortEx	portex_2.12-4.0.8.jar	4.0.8
JSONLD Java :: Core	jsonld-java-0.13.4.jar	0.13.4
json-schema-core	json-schema-core-1.2.14.jar	1.2.14
msg-simple	msg-simple-1.2.jar	1.2
uri-template	uri-template-0.10.jar	0.10
curvesapi	curvesapi-1.08.jar	1.08
zstd-jni	zstd-jni-1.5.2-4.jar	1.5.2-4
Package URL	packageurl-java-1.5.0.jar	1.5.0

Weakness

CWE-913

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-8qp2-79w8-8586	GitHub Enterprise before 20120304 does not properly restrict the use of a hash to provide values for a model's attributes, which allows remote attackers to set the public_key[user_id] value via a modified URL for the public-key update form, related to a "mass assignment" vulnerability.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.30 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 29.69 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2012-0815

Description

The headerVerifyInfo function in lib/header.c in RPM before 4.9.1.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a negative value in a region offset of a package header, which is not properly handled in a numeric range comparison.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2012-0815

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-189

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.8	AV:N/AC:M/Au:N/C:P/I:P/A:P	Medium

Advisories

Doc. Identifier: \${document.id}

Alerts

ld	Summary	Create Date	Update Date
CERT-EU-2012-0126	VMware vSphere and vCOps updates to third party libraries	2012-11-16	2012-11-16
GHSA-6grx-55mc-2wmq	The headerVerifyInfo function in lib/header.c in RPM before 4.9.1.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a negative value in a region offset of a package header, which is not properly handled in a numeric range comparison.	2022-05-14	2022-05-14

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 5.76 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 6.39 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2012-0061

Description

The headerLoad function in lib/header.c in RPM before 4.9.1.3 does not properly validate region tags, which allows user-assisted remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large region size in a package header.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2012-0061

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-20

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.8	AV:N/AC:M/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
CERT-EU-2012-0126	VMware vSphere and vCOps updates to third party libraries	2012-11-16	2012-11-16
GHSA-v3v4-hffr-vr89	The headerLoad function in lib/header.c in RPM before 4.9.1.3 does not properly validate region tags, which allows user-assisted remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large region size in a package header.	2022-05-04	2022-05-04

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 4.55 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 7.21 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2012-0060

Doc. Identifier: \${document.id}

Description

RPM before 4.9.1.3 does not properly validate region tags, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an invalid region tag in a package header to the (1) headerLoad, (2) rpmReadSignature, or (3) headerVerify function.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2012-0060

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-20

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.8	AV:N/AC:M/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
CERT-EU-2012-0126	VMware vSphere and vCOps updates to third party libraries	2012-11-16	2012-11-16
GHSA-j6wj-cqmg-hvcm	RPM before 4.9.1.3 does not properly validate region tags, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an invalid region tag in a package header to the (1) headerLoad, (2) rpmReadSignature, or (3) headerVerify function.	2022-05-04	2022-05-04

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 4.55 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 7.21 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2011-3378

Description

RPM 4.4.x through 4.9.x, probably before 4.9.1.2, allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via an rpm package with crafted headers and offsets that are not properly handled when a package is queried or installed, related to (1) the regionSwab function, (2) the headerLoad function, and (3) multiple functions in rpmio/rpmpgp.c.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2011-3378

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-94

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	9.3	AV:N/AC:M/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-34ff-v8wx-w9f5	RPM 4.4.x through 4.9.x, probably before 4.9.1.2, allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via an rpm package with crafted headers and offsets that are not properly handled when a package is queried or installed, related to (1) the regionSwab function, (2) the headerLoad function, and (3) multiple functions in rpmio/rpmpgp.c.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi} Page 118 of 290 Doc. Date: \${document.date_

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 6.39 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 6.10 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2010-2199

Description

lib/fsm.c in RPM 4.8.0 and earlier does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade or deletion of the file in an RPM package removal, which might allow local users to bypass intended access restrictions by creating a hard link to a vulnerable file that has a POSIX ACL, a related issue to CVE-2010-2059.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2010-2199

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-264

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.2	AV:L/AC:L/Au:N/C:C/I:C/A:C	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-7v29-vf8p-2rvp	lib/fsm.c in RPM 4.8.0 and earlier does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade or deletion of the file in an RPM package removal, which might allow local users to bypass intended access restrictions by creating a hard link to a vulnerable file that has a POSIX ACL, a related issue to CVE-2010-2059.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2010-2198

Description

lib/fsm.c in RPM 4.8.0 and earlier does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade or deletion of the file in an RPM package removal, which might allow local users to gain privileges or bypass intended access restrictions by creating a hard link to a vulnerable file that has (1) POSIX file capabilities or (2) SELinux context information, a related issue to CVE-2010-2059.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2010-2198

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-264

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.2	AV:L/AC:L/Au:N/C:C/I:C/A:C	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-fw46-vp2w-pvxq	lib/fsm.c in RPM 4.8.0 and earlier does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade or deletion of the file in an RPM package removal, which might allow local users to gain privileges or bypass intended access restrictions by creating a hard link to a vulnerable file that has (1) POSIX file capabilities or (2) SELinux context information, a related issue to CVE-2010-2059.	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

	•
Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2010-2197

Description

rpmbuild in RPM 4.8.0 and earlier does not properly parse the syntax of spec files, which allows user-assisted remote attackers to remove home directories via vectors involving a ;~ (semicolon tilde) sequence in a Name tag.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2010-2197

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-264

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-6gj2-w23f-chf3	rpmbuild in RPM 4.8.0 and earlier does not properly parse the syntax of spec files, which allows user-assisted remote attackers to remove home directories via vectors involving a ; \sim (semicolon tilde) sequence in a Name tag.	2022-05-17	2022-05-17

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:N/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.26 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 33.31 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2010-2059

Description

lib/fsm.c in RPM 4.8.0 and unspecified 4.7.x and 4.6.x versions, and RPM before 4.4.3, does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade, which might allow local users to gain privileges by creating a hard link to a vulnerable (1) setuid or (2) setgid file.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2010-2059

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-264

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.2	AV:L/AC:L/Au:N/C:C/I:C/A:C	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-f3f6-q22p-8fh5	lib/fsm.c in RPM 4.8.0 and unspecified 4.7.x and 4.6.x versions, and RPM before 4.4.3, does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade, which might allow local users to gain privileges by creating a hard link to a vulnerable (1) setuid or (2) setgid file.	2022-05-14	2022-05-14

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 88.55 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2009-3014

Description

Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1 pre; SeaMonkey 1.1.17; and Mozilla 1.7.x and earlier do not properly handle javascript: URIs in HTML links within 302 error documents sent from web servers, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Location HTTP response header or (2) specifying the content of a Location HTTP response header.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2009-3014

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Weakness

CWE-79

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Doc. Identifier: \${document.id}

Alerts

ld	Summary	Create Date	Update Date
GHSA-xw9p-2mr3-g9mx	Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1 pre; SeaMonkey 1.1.17; and Mozilla 1.7.x and earlier do not properly handle javascript: URIs in HTML links within 302 error documents sent from web servers, which allows user-assisted remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Location HTTP response header or (2) specifying the content of a Location HTTP response header.	2022-05-02	2022-05-02

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.19 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 42.74 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2009-3010

Description

Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1 pre; SeaMonkey 1.1.17; and Mozilla 1.7.x and earlier do not properly block data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header. NOTE: in some product versions, the JavaScript executes outside of the context of the HTTP site.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2009-3010

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Weakness

CWE-79

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-mv6q-6xwq-rrw9	Mozilla Firefox 3.0.13 and earlier, 3.5, 3.6 a1 pre, and 3.7 a1 pre; SeaMonkey 1.1.17; and Mozilla 1.7.x and earlier do not properly block data: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header that contains JavaScript sequences in a data:text/html URI or (2) entering a data:text/html URI with JavaScript sequences when specifying the content of a Refresh header. NOTE: in some product versions, the JavaScript executes outside of the context of the HTTP site.	2022-05-02	2022-05-02

Assessment

Summary

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.18 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 44.17 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2009-1251

Description

Heap-based buffer overflow in the cache manager in the client in OpenAFS 1.0 through 1.4.8 and 1.5.0 through 1.5.58 on Unix platforms allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via an RX response containing more data than specified in a request, related to use of XDR arrays.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2009-1251

Affected Components

Component	Artifact Id	Version
Netty/Transport/Native/Unix/Common	netty-transport-native-unix-common-4.1.110.Final.	4.1.110.Final

Weakness

CWE-119

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-2xj8-3jr2-7qw3	Heap-based buffer overflow in the cache manager in the client in OpenAFS 1.0 through 1.4.8 and 1.5.0 through 1.5.58 on Unix platforms allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via an RX response containing more data than specified in a request, related to use of XDR arrays.	2022-05-02	2022-05-02

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 16.27 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 3.85 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.

Doc. Identifier: \${document.id}

\${document.name} Page 127 of 290 Doc. Version: \${document.versi}
Doc. Date: \${document.date_

Criteria	Explanation
Assessment	The vulnerability status is in review .

CVE-2008-6161

Description

Cross-site scripting (XSS) vulnerability in WOW Raid Manager (WRM) before 3.5.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2008-6161

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-79

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-682j-rhpc-phrj	Cross-site scripting (XSS) vulnerability in WOW Raid Manager (WRM) before 3.5.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2022-05-17	2022-05-17

Assessment

Summary

		$\overline{}$
Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.19 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 42.07 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2008-2503

Description

Buffer overflow in Uploadlist in eMule X-Ray before 1.4 has unknown impact and remote attack vectors.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2008-2503

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-119

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	9.3	AV:N/AC:M/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-jxq6-p7m9-896m	Buffer overflow in Uploadlist in eMule X-Ray before 1.4 has unknown impact and remote attack vectors.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi} Page 129 of 290 Doc. Date: \${document.date_

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.19 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 42.65 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2008-2298

Description

Admin.php in Web Slider 0.6 allows remote attackers to bypass authentication and gain privileges by setting the admin cookie to 1.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2008-2298

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-287

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-39wm-cmp6-6mjc	Admin.php in Web Slider 0.6 allows remote attackers to bypass authentication and gain privileges by setting the admin cookie to 1.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.86 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 8.93 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2008-0501

Description

Directory traversal vulnerability in phpMyClub 0.0.1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page_courante parameter to the top-level URI.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2008-0501

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-22

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-q7mg-4q42-3h7f	Directory traversal vulnerability in phpMyClub 0.0.1 allows remote attackers to include and execute arbitrary local files via a (dot dot) in the page_courante parameter to the top-level URI.	2022-05-01	2022-05-01

Assessment

Summary

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:P/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.95 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 16.18 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2007-6640

Description

Creammonkey 0.9 through 1.1 and GreaseKit 1.2 through 1.3 does not properly prevent access to dangerous functions, which allows remote attackers to read the configuration, modify the configuration, or send an HTTP request via the (1) GM_addStyle, (2) GM_log, (3) GM_openInTab, (4) GM_setValue, (5) GM_getValue, or (6) GM_xmlhttpRequest function within a web page on which a userscript is configured.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2007-6640

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-264

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-jmrg-23pg-v7hm	Creammonkey 0.9 through 1.1 and GreaseKit 1.2 through 1.3 does not properly prevent access to dangerous functions, which allows remote attackers to read the configuration, modify the configuration, or send an HTTP request via the (1) GM_addStyle, (2) GM_log, (3) GM_openInTab, (4) GM_setValue, (5) GM_getValue, or (6) GM_xmlhttpRequest function within a web page on which a userscript is configured.	2022-05-01	2022-05-01

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default	No alayoted priority
Delauit	No elevated priority

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.46 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 23.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2007-4039

Description

Argument injection vulnerability involving Mozilla, when certain URIs are registered, allows remote attackers to conduct cross-browser scripting attacks and execute arbitrary commands via shell metacharacters in an unspecified URI, which are inserted into the command line when invoking the handling process, a similar issue to CVE-2007-3670.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2007-4039

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Weakness

CWE-79

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-5qrv-2vjc-xwcq	Argument injection vulnerability involving Mozilla, when certain URIs are registered, allows remote attackers to conduct cross-browser scripting attacks and execute arbitrary commands via shell metacharacters in an unspecified URI, which are inserted into the command line when invoking the handling process, a similar issue to CVE-2007-3670.	2022-05-01	2022-05-01

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.09 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 59.28 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.

Criteria	Explanation
Assessment	The vulnerability status is insignificant .

CVE-2007-1794

Description

The Javascript engine in Mozilla 1.7 and earlier on Sun Solaris 8, 9, and 10 might allow remote attackers to execute arbitrary code via vectors involving garbage collection that causes deletion of a temporary object that is still being used. NOTE: this issue might be related to CVE-2006-3805.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2007-1794

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-whc6-8wvp-96v2	The Javascript engine in Mozilla 1.7 and earlier on Sun Solaris 8, 9, and 10 might allow remote attackers to execute arbitrary code via vectors involving garbage collection that causes deletion of a temporary object that is still being used. NOTE: this issue might be related to CVE-2006-3805.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.60 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 12.08 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2007-1466

Description

Integer overflow in the WP6GeneralTextPacket::_readContents function in WordPerfect Document importer/exporter (libwpd) before 0.8.9 allows user-assisted remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted WordPerfect file, a different vulnerability than CVE-2007-0002.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2007-1466

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-189

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.8	AV:N/AC:M/Au:N/C:P/I:P/A:P	Medium

Advisories

Doc. Identifier: \${document.id}

Alerts

ld	Summary	Create Date	Update Date
GHSA-mc39-g53r-8cq4	Integer overflow in the WP6GeneralTextPacket::_readContents function in WordPerfect Document importer/exporter (libwpd) before 0.8.9 allows user-assisted remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted WordPerfect file, a different vulnerability than CVE-2007-0002.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 14.85 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 4.02 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2007-1157

Description

Cross-site request forgery (CSRF) vulnerability in jmx-console/HtmlAdaptor in JBoss allows remote attackers to perform privileged actions as administrators via certain MBean operations, a different vulnerability than CVE-2006-3733.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2007-1157

Affected Components

Component	Artifact Id	Version
CDI APIs	cdi-api-1.2.jar	1.2

Weakness

CWE-352

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.6	AV:N/AC:H/Au:N/C:C/I:C/A:C	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-r86m-hxp8-3mvw	Cross-site request forgery (CSRF) vulnerability in jmx-console/ HtmlAdaptor in JBoss allows remote attackers to perform privileged actions as administrators via certain MBean operations, a different vulnerability than CVE-2006-3733.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

	o o o o o o o o o o o o o o o o o
Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.23 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 37.75 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2007-1137

Description

putmail.py in Putmail before 1.4 does not detect when a user attempts to use TLS with a server that does not support it, which causes putmail.py to send the username and password in plaintext while the user believes encryption is in use, and allows remote attackers to obtain sensitive information.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2007-1137

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-x927-rp8j-62cg	putmail.py in Putmail before 1.4 does not detect when a user attempts to use TLS with a server that does not support it, which causes putmail.py to send the username and password in plaintext while the user believes encryption is in use, and allows remote attackers to obtain sensitive information.	2022-05-01	2022-05-01

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.91 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 16.58 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2006-6498

Description

Multiple unspecified vulnerabilities in the JavaScript engine for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, SeaMonkey before 1.0.7, and Mozilla 1.7 and probably earlier on Solaris, allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via unknown impact and attack vectors.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2006-6498

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.8	AV:N/AC:M/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-jmfp-6hwg-w7qf	Multiple unspecified vulnerabilities in the JavaScript engine for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, SeaMonkey before 1.0.7, and Mozilla 1.7 and probably earlier on Solaris, allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via unknown impact and attack vectors.	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Due (8.0 from base score 6.8)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 74.12 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 1.78 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2006-5562

Description

PHP remote file inclusion vulnerability in include/database.php in SourceForge (aka alexandria) 1.0.4 allows remote attackers to execute arbitrary PHP code via the sys_dbtype parameter.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2006-5562

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-wxm5-2gcr-wvxp	PHP remote file inclusion vulnerability in include/database.php in SourceForge (aka alexandria) 1.0.4 allows remote attackers to execute arbitrary PHP code via the sys_dbtype parameter.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 5.05 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 6.82 % of all scored vulnerabilities.

Criteria	Explanation
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2006-1547

Description

ActionForm in Apache Software Foundation (ASF) Struts before 1.2.9 with BeanUtils 1.7 allows remote attackers to cause a denial of service via a multipart/form-data encoded form with a parameter name that references the public getMultipartRequestHandler method, which provides further access to elements in the CommonsMultipartRequestHandler implementation and BeanUtils.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2006-1547

Affected Components

Component	Artifact Id	Version
	commons-beanutils-1.7.0.jar	1.7.0

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	7.8	AV:N/AC:L/Au:N/C:N/I:N/A:C	High

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-7qwv-cwgj-c8rj	Improper Input Validation in Apache Struts	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (9.5 from base score 7.5)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 8.92 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 5.18 % of all scored vulnerabilities.
KEV	This vulnerability, affecting Apache Struts 1 , has been confirmed to have been exploited in the wild . Summary: Apache Struts 1 ActionForm Denial-of-Service Vulnerability. Apply updates per vendor instructions. Notes: https://nvd.nist.gov/vuln/detail/CVE-2006-1547 Due Date: 2022-07-21 Publish Date: 2022-01-21
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2006-0496

Description

Cross-site scripting (XSS) vulnerability in Mozilla 1.7.12 and possibly earlier, Mozilla Firefox 1.0.7 and possibly earlier, and Netscape 8.1 and possibly earlier, allows remote attackers to inject arbitrary web script or HTML via the -moz-binding (Cascading Style Sheets) CSS property, which does not require that the style sheet have the same origin as the web page, as demonstrated by the compromise of a large number of LiveJournal accounts.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2006-0496

Affected Components

Doc. Identifier: \${document.id}

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-747m-cwr6-qmx3	Cross-site scripting (XSS) vulnerability in Mozilla 1.7.12 and possibly earlier, Mozilla Firefox 1.0.7 and possibly earlier, and Netscape 8.1 and possibly earlier, allows remote attackers to inject arbitrary web script or HTML via the -moz-binding (Cascading Style Sheets) CSS property, which does not require that the style sheet have the same origin as the web page, as demonstrated by the compromise of a large number of LiveJournal accounts.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant Elevated Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Elevated (6.0 from base score 4.3)

	·
Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 91.12 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 1.00 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-4889

Description

lib/fsm.c in RPM before 4.4.3 does not properly reset the metadata of an executable file during deletion of the file in an RPM package removal, which might allow local users to gain privileges by creating a hard link to a vulnerable (1) setuid or (2) setgid file, a related issue to CVE-2010-2059.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-4889

Affected Components

Component	Artifact Id	Version
	org.eclipse.packagedrone.utils.rpm-0.14.6.jar	0.14.6

Weakness

CWE-264

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.2	AV:L/AC:L/Au:N/C:C/I:C/A:C	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-pfqv-vjx4-pmxj	lib/fsm.c in RPM before 4.4.3 does not properly reset the metadata of an executable file during deletion of the file in an RPM package removal, which might allow local users to gain privileges by creating a hard link to a vulnerable (1) setuid or (2) setgid file, a related issue to CVE-2010-2059.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

snmp_api.c in snmpd in Net-SNMP 5.2.x before 5.2.2, 5.1.x before 5.1.3, and 5.0.x before 5.0.10.2, when running in master agentx mode, allows remote attackers to cause a denial of service (crash) by causing a particular TCP disconnect, which triggers a free of an incorrect variable, a different vulnerability than CVE-2005-2177.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-4837

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-16

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-m3xm-f262-69qm	snmp_api.c in snmpd in Net-SNMP 5.2.x before 5.2.2, 5.1.x before 5.1.3, and 5.0.x before 5.0.10.2, when running in master agentx mode, allows remote attackers to cause a denial of service (crash) by causing a particular TCP disconnect, which triggers a free of an incorrect variable, a different vulnerability than CVE-2005-2177.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 13.54 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 4.20 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

Firefox and Mozilla can associate a cookie with multiple domains when the DNS resolver has a non-root domain in its search list, which allows remote attackers to trick a user into accepting a cookie for a hostname formed via search-list expansion of the hostname entered by the user, or steal a cookie for an expanded hostname, as demonstrated by an attacker who operates an ap1.com Internet web site to steal cookies associated with an ap1.com.example.com intranet web site.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-4685

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Medium

Advisories

Doc. Identifier: \${document.id}

Alerts

ld	Summary	Create Date	Update Date
GHSA-qx3r-96cr-cwr5	Firefox and Mozilla can associate a cookie with multiple domains when the DNS resolver has a non-root domain in its search list, which allows remote attackers to trick a user into accepting a cookie for a hostname formed via search-list expansion of the hostname entered by the user, or steal a cookie for an expanded hostname, as demonstrated by an attacker who operates an ap1.com Internet web site to steal cookies associated with an ap1.com.example.com intranet web site.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.22 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 39.06 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-3896

Description

Mozilla allows remote attackers to cause a denial of service (CPU consumption) via a Javascript BODY onload event that calls the window function.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-3896

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.8	AV:N/AC:L/Au:N/C:N/I:N/A:C	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-f389-88pf-8hp7	Mozilla allows remote attackers to cause a denial of service (CPU consumption) via a Javascript BODY onload event that calls the window function.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.32 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 28.80 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-2270

Description

Firefox before 1.0.5 and Mozilla before 1.7.9 does not properly clone base objects, which allows remote attackers to execute arbitrary code by navigating the prototype chain to reach a privileged object.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-2270

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-jgwp-9p3p-4h7j	Firefox before 1.0.5 and Mozilla before 1.7.9 does not properly clone base objects, which allows remote attackers to execute arbitrary code by navigating the prototype chain to reach a privileged object.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 8.92 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 5.18 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-2269

Description

Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 does not properly verify the associated types of DOM node names within the context of their namespaces, which allows remote attackers to modify certain tag properties, possibly leading to execution of arbitrary script or code, as demonstrated using an XHTML document with IMG tags with custom properties ("XHTML node spoofing").

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-2269

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-cxw5-72vp-8h54	Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 does not properly verify the associated types of DOM node names within the context of their namespaces, which allows remote attackers to modify certain tag properties, possibly leading to execution of arbitrary script or code, as demonstrated using an XHTML document with IMG tags with custom properties ("XHTML node spoofing").	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 9.56 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 5.00 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

Firefox before 1.0.5 and Mozilla before 1.7.9 does not clearly associate a Javascript dialog box with the web page that generated it, which allows remote attackers to spoof a dialog box from a trusted site and facilitates phishing attacks, aka the "Dialog Origin Spoofing Vulnerability."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-2268

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-3937-9m84-64gp	Firefox before 1.0.5 and Mozilla before 1.7.9 does not clearly associate a Javascript dialog box with the web page that generated it, which allows remote attackers to spoof a dialog box from a trusted site and facilitates phishing attacks, aka the "Dialog Origin Spoofing Vulnerability."	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Low
Insignificant	Default	Low

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.

Criteria	Explanation
EPSS	This vulnerability has a 0.51 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 22.74 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Firefox before 1.0.5 and Mozilla before 1.7.9 allows a child frame to call top.focus and other methods in a parent frame, even when the parent is in a different domain, which violates the same origin policy and allows remote attackers to steal sensitive information such as cookies and passwords from web sites whose child frames do not verify that they are in the same domain as their parents.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-2266

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-gp89-32gv-6hww	Firefox before 1.0.5 and Mozilla before 1.7.9 allows a child frame to call top.focus and other methods in a parent frame, even when the parent is in a different domain, which violates the same origin policy and allows remote attackers to steal sensitive information such as cookies and passwords from web sites whose child frames do not verify that they are in the same domain as their parents.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant Default Me

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.31 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 13.56 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-2265

Description

Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 and 7.2 allows remote attackers to cause a denial of service (access violation and crash), and possibly execute arbitrary code, by calling InstallVersion.compareTo with an object instead of a string.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-2265

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-5pgg-4c5c-9j5p	Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 and 7.2 allows remote attackers to cause a denial of service (access violation and crash), and possibly execute arbitrary code, by calling InstallVersion.compareTo with an object instead of a string.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant Elevated Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Elevated (6.9 from base score 5.0)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 96.72 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 0.29 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-2263

Description

The InstallTrigger.install method in Firefox before 1.0.5 and Mozilla before 1.7.9 allows remote attackers to execute a callback function in the context of another domain by forcing a page navigation after the install method has been called, which causes the callback to be run in the context of the new page and results in a same origin violation.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-2263

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versions}Page 155 of 290Doc. Date: \${document.date_

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-5v66-4mqr-49xj	The InstallTrigger.install method in Firefox before 1.0.5 and Mozilla before 1.7.9 allows remote attackers to execute a callback function in the context of another domain by forcing a page navigation after the install method has been called, which causes the callback to be run in the context of the new page and results in a same origin violation.	2022-05-01	2022-05-01

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

	• •
Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.46 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 9.58 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-2261

Description

Firefox before 1.0.5, Thunderbird before 1.0.5, Mozilla before 1.7.9, Netscape 8.0.2, and K-Meleon 0.9 runs XBL scripts even when Javascript has been disabled, which makes it easier for remote attackers to bypass such protection.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-2261

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-j45r-pcwj-8g72	Firefox before 1.0.5, Thunderbird before 1.0.5, Mozilla before 1.7.9, Netscape 8.0.2, and K-Meleon 0.9 runs XBL scripts even when Javascript has been disabled, which makes it easier for remote attackers to bypass such protection.	2022-05-01	2022-05-01

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 4.40 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 7.34 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-2260

Description

The browser user interface in Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 and 7.2 does not properly distinguish between user-generated events and untrusted synthetic events, which makes it easier for remote attackers to perform dangerous actions that normally could only be performed manually by the user.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-2260

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-wm6x-mrp3-f56m	The browser user interface in Firefox before 1.0.5, Mozilla before 1.7.9, and Netscape 8.0.2 and 7.2 does not properly distinguish between usergenerated events and untrusted synthetic events, which makes it easier for remote attackers to perform dangerous actions that normally could only be performed manually by the user.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.31 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 9.92 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

A regression error in Firefox 1.0.3 and Mozilla 1.7.7 allows remote attackers to inject arbitrary Javascript from one page into the frameset of another site, aka the frame injection spoofing vulnerability, a re-introduction of a vulnerability that was originally identified and addressed by CVE-2004-0718.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1937

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-ffxc-32xj-v3rp	A regression error in Firefox 1.0.3 and Mozilla 1.7.7 allows remote attackers to inject arbitrary Javascript from one page into the frameset of another site, aka the frame injection spoofing vulnerability, a reintroduction of a vulnerability that was originally identified and addressed by CVE-2004-0718.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Low

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.

Doc. Identifier: \${document.id}

\${document.name} Page 159 of 290 Doc. Version: \${document.versic Doc. Date: \${document.date_

Criteria	Explanation
EPSS	This vulnerability has a 0.29 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 30.07 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Firefox before 1.0.4 and Mozilla Suite before 1.7.8 do not properly limit privileges of Javascript eval and Script objects in the calling context, which allows remote attackers to conduct unauthorized activities via "non-DOM property overrides," a variant of CVE-2005-1160.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1532

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Weakness

CWE-264

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-ffv2-fj33-mvch	Firefox before 1.0.4 and Mozilla Suite before 1.7.8 do not properly limit privileges of Javascript eval and Script objects in the calling context, which allows remote attackers to conduct unauthorized activities via "non-DOM property overrides," a variant of CVE-2005-1160.	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Due (8.2 from base score 7.5)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 56.57 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 2.21 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-1531

Description

Firefox before 1.0.4 and Mozilla Suite before 1.7.8 does not properly implement certain security checks for script injection, which allows remote attackers to execute script via "Wrapped" javascript: URLs, as demonstrated using (1) a javascript: URL in a view-source: URL, (2) a javascript: URL in a jar: URL, or (3) "a nested variant."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1531

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-q7v5-vf67-fpfr	Firefox before 1.0.4 and Mozilla Suite before 1.7.8 does not properly implement certain security checks for script injection, which allows remote attackers to execute script via "Wrapped" javascript: URLs, as demonstrated using (1) a javascript: URL in a view-source: URL, (2) a javascript: URL in a jar: URL, or (3) "a nested variant."	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.57 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 21.55 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-1160

Description

The privileged "chrome" UI code in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to gain privileges by overriding certain properties or methods of DOM nodes, as demonstrated using multiple attacks involving the eval function or the Script object.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1160

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.1	AV:N/AC:H/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-r5gq-7c27-jhm8	The privileged "chrome" UI code in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to gain privileges by overriding certain properties or methods of DOM nodes, as demonstrated using multiple attacks involving the eval function or the Script object.	2022-05-03	2022-05-03

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation			
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:P/I:P/A:P			
Keywords	No keyword sets matched.			
EPSS	This vulnerability has a 0.49 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 23.29 % of all scored vulnerabilities.			
KEV	This vulnerability has not been confirmed to have been exploited in the wild.			
EOL	No end-of-life (EOL) information available.			
Assessment	The vulnerability status is insignificant .			

CVE-2005-1159

Description

The native implementations of InstallTrigger and other functions in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 do not properly verify the types of objects being accessed, which causes the Javascript interpreter to continue execution at the wrong memory address, which may allow attackers to cause a denial of service (application crash) and possibly execute arbitrary code by passing objects of the wrong type.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1159

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Doc. Identifier: \${document.id} \${document.name} Doc. Version: \${document.versi} Page 163 of 290 Doc. Date: \${document.date_

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-65q8-rprw-c44f	The native implementations of InstallTrigger and other functions in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 do not properly verify the types of objects being accessed, which causes the Javascript interpreter to continue execution at the wrong memory address, which may allow attackers to cause a denial of service (application crash) and possibly execute arbitrary code by passing objects of the wrong type.	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.47 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 12.73 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-1157

Description

Firefox before 1.0.3, Mozilla Suite before 1.7.7, and Netscape 7.2 allows remote attackers to replace existing search plugins with malicious ones using sidebar.addSearchEngine and the same filename as the target engine, which may not be displayed in the GUI, which could then be used to execute malicious script, aka "Firesearching 2."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1157

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

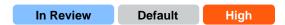
Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-8hfq-wv6x-73v6	Firefox before 1.0.3, Mozilla Suite before 1.7.7, and Netscape 7.2 allows remote attackers to replace existing search plugins with malicious ones using sidebar.addSearchEngine and the same filename as the target engine, which may not be displayed in the GUI, which could then be used to execute malicious script, aka "Firesearching 2."	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.34 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 13.37 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

Firefox before 1.0.3, Mozilla Suite before 1.7.7, and Netscape 7.2 allows remote attackers to execute arbitrary script and code via a new search plugin using sidebar.addSearchEngine, aka "Firesearching 1."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1156

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-p7cq-vpx5-5pp5	Firefox before 1.0.3, Mozilla Suite before 1.7.7, and Netscape 7.2 allows remote attackers to execute arbitrary script and code via a new search plugin using sidebar.addSearchEngine, aka "Firesearching 1."	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.94 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 16.33 % of all scored vulnerabilities.

Criteria	Explanation
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

The favicon functionality in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to execute arbitrary code via a <LINK rel="icon"> tag with a javascript: URL in the href attribute, aka "Firelinking."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1155

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Weakness

CWE-94

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-5f3p-wqh5-33m5	The favicon functionality in Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to execute arbitrary code via a <link rel="icon"/> tag with a javascript: URL in the href attribute, aka "Firelinking."	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (9.2 from base score 7.5)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 89.66 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 1.11 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-1154

Description

Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to execute arbitrary script in other domains via a setter function for a variable in the target domain, which is executed when the user visits that domain, aka "Cross-site scripting through global scope pollution."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1154

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-xrcj-fc8v-w45w	Firefox before 1.0.3 and Mozilla Suite before 1.7.7 allows remote attackers to execute arbitrary script in other domains via a setter function for a variable in the target domain, which is executed when the user visits that domain, aka "Cross-site scripting through global scope pollution."	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.90 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 16.66 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-1153

Description

Firefox before 1.0.3 and Mozilla Suite before 1.7.7, when blocking a popup, allows remote attackers to execute arbitrary code via a javascript: URL that is executed when the user selects the "Show javascript" option.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-1153

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-9j3v-w638-mx3p	Firefox before 1.0.3 and Mozilla Suite before 1.7.7, when blocking a popup, allows remote attackers to execute arbitrary code via a javascript: URL that is executed when the user selects the "Show javascript" option.	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 3.53 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 8.11 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-0593

Description

Firefox before 1.0.1 and Mozilla before 1.7.6 allows remote attackers to spoof the SSL "secure site" lock icon via (1) a web site that does not finish loading, which shows the lock of the previous site, (2) a non-HTTP server that uses SSL, which causes the lock to be displayed when the SSL handshake is completed, or (3) a URL that generates an HTTP 204 error, which updates the icon and location information but does not change the display of the original site.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0593

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-74mv-jc74-mg2v	Firefox before 1.0.1 and Mozilla before 1.7.6 allows remote attackers to spoof the SSL "secure site" lock icon via (1) a web site that does not finish loading, which shows the lock of the previous site, (2) a non-HTTP server that uses SSL, which causes the lock to be displayed when the SSL handshake is completed, or (3) a URL that generates an HTTP 204 error, which updates the icon and location information but does not change the display of the original site.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant Default	Low
-----------------------	-----

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.29 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 30.35 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0592

Description

Heap-based buffer overflow in the UTF8ToNewUnicode function for Firefox before 1.0.1 and Mozilla before 1.7.6 might allow remote attackers to cause a denial of service (crash) or execute arbitrary code via invalid sequences in a UTF8 encoded string that result in a zero length value.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0592

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-3fwv-8g5j-79jx	Heap-based buffer overflow in the UTF8ToNewUnicode function for Firefox before 1.0.1 and Mozilla before 1.7.6 might allow remote attackers to cause a denial of service (crash) or execute arbitrary code via invalid sequences in a UTF8 encoded string that result in a zero length value.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.11 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 10.42 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-0590

Description

The installation confirmation dialog in Firefox before 1.0.1, Thunderbird before 1.0.1, and Mozilla before 1.7.6 allows remote attackers to use InstallTrigger to spoof the hostname of the host performing the installation via a long "user:pass" sequence in the URL, which appears before the real hostname.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0590

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-mq4v-fvj7-qhmj	The installation confirmation dialog in Firefox before 1.0.1, Thunderbird before 1.0.1, and Mozilla before 1.7.6 allows remote attackers to use InstallTrigger to spoof the hostname of the host performing the installation via a long "user:pass" sequence in the URL, which appears before the real hostname.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.28 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 30.53 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Firefox before 1.0.1 and Mozilla before 1.7.6 does not restrict xsl:include and xsl:import tags in XSLT stylesheets to the current domain, which allows remote attackers to determine the existence of files on the local system.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0588

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-g63h-wr5c- mmgm	Firefox before 1.0.1 and Mozilla before 1.7.6 does not restrict xsl:include and xsl:import tags in XSLT stylesheets to the current domain, which allows remote attackers to determine the existence of files on the local system.	2022-05-01	2022-05-01

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.28 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 13.68 % of all scored vulnerabilities.

Doc. Identifier: \${document.id}

\${document.name} Page 174 of 290 Doc. Version: \${document.versic Doc. Date: \${document.date_

Criteria	Explanation
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Firefox before 1.0.1 and Mozilla before 1.7.6 allows remote malicious web sites to spoof the extensions of files to download via the Content-Disposition header, which could be used to trick users into downloading dangerous content.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0586

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-wrw4-477q-3qjh	Firefox before 1.0.1 and Mozilla before 1.7.6 allows remote malicious web sites to spoof the extensions of files to download via the Content-Disposition header, which could be used to trick users into downloading dangerous content.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Low
---------------	---------	-----

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.45 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 24.13 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Firefox before 1.0.1 and Mozilla before 1.7.6 truncates long sub-domains or paths for display, which may allow remote malicious web sites to spoof legitimate sites and facilitate phishing attacks.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0585

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-cxhx-r8q3-rf4p	Firefox before 1.0.1 and Mozilla before 1.7.6 truncates long sub-domains or paths for display, which may allow remote malicious web sites to spoof legitimate sites and facilitate phishing attacks.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Low

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.27 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 31.38 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0584

Description

Firefox before 1.0.1 and Mozilla before 1.7.6, when displaying the HTTP Authentication dialog, do not change the focus to the tab that generated the prompt, which could facilitate spoofing and phishing attacks.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0584

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

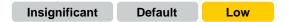
Doc. Identifier: \${document.id}

Alerts

ld	Summary	Create Date	Update Date
GHSA-v9x2-68hw-cwxx	Firefox before 1.0.1 and Mozilla before 1.7.6, when displaying the HTTP Authentication dialog, do not change the focus to the tab that generated the prompt, which could facilitate spoofing and phishing attacks.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.09 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 60.39 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0578

Description

Firefox before 1.0.1 and Mozilla Suite before 1.7.6 use a predictable filename for the plugin temporary directory, which allows local users to delete arbitrary files of other users via a symlink attack on the plugtmp directory.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0578

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.1	AV:L/AC:L/Au:N/C:N/I:N/A:P	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-7352-x97x-grpg	Firefox before 1.0.1 and Mozilla Suite before 1.7.6 use a predictable filename for the plugin temporary directory, which allows local users to delete arbitrary files of other users via a symlink attack on the plugtmp directory.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Low
---------------	---------	-----

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0401

Description

FireFox 1.0.1 and Mozilla before 1.7.6 do not sufficiently address all attack vectors for loading chrome files and hijacking drag and drop events, which allows remote attackers to execute arbitrary XUL code by tricking a user into dragging a scrollbar, a variant of CVE-2005-0527, aka "Firescrolling 2."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0401

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.1	AV:N/AC:H/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-p4xc-fq3x-cx45	FireFox 1.0.1 and Mozilla before 1.7.6 do not sufficiently address all attack vectors for loading chrome files and hijacking drag and drop events, which allows remote attackers to execute arbitrary XUL code by tricking a user into dragging a scrollbar, a variant of CVE-2005-0527, aka "Firescrolling 2."	2022-05-01	2022-05-01

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 3.95 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 7.68 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0399

Description

Heap-based buffer overflow in GIF2.cpp in Firefox before 1.0.2, Mozilla before to 1.7.6, and Thunderbird before 1.0.2, and possibly other applications that use the same library, allows remote attackers to execute arbitrary code via a GIF image with a crafted Netscape extension 2 block and buffer size.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0399

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.1	AV:N/AC:H/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-x75c-2774-mpv3	Heap-based buffer overflow in GIF2.cpp in Firefox before 1.0.2, Mozilla before to 1.7.6, and Thunderbird before 1.0.2, and possibly other applications that use the same library, allows remote attackers to execute arbitrary code via a GIF image with a crafted Netscape extension 2 block and buffer size.	2022-05-03	2022-05-03

Assessment

Summary

Insignificant	Elevated	Medium
moignineant	Licvatca	Mediam

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Elevated (6.9 from base score 5.1)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 91.99 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 0.94 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0149

Description

Thunderbird 0.6 through 0.9 and Mozilla 1.7 through 1.7.3 does not obey the network.cookie.disableCookieForMailNews preference, which could allow remote attackers to bypass the user's intended privacy and security policy by using cookies in e-mail messages.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0149

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-2x58-77jw-wgpw	Thunderbird 0.6 through 0.9 and Mozilla 1.7 through 1.7.3 does not obey the network.cookie.disableCookieForMailNews preference, which could allow remote attackers to bypass the user's intended privacy and security policy by using cookies in e-mail messages.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Medium
moigimiount	Doidait	mearani

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versions}Page 182 of 290Doc. Date: \${document.date_

Criteria	Explanation
EPSS	This vulnerability has a 0.34 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 27.90 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0147

Description

Firefox before 1.0 and Mozilla before 1.7.5, when configured to use a proxy, respond to 407 proxy auth requests from arbitrary servers, which allows remote attackers to steal NTLM or SPNEGO credentials.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0147

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-25p3-2r5q-956q	Firefox before 1.0 and Mozilla before 1.7.5, when configured to use a proxy, respond to 407 proxy auth requests from arbitrary servers, which allows remote attackers to steal NTLM or SPNEGO credentials.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.38 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 26.14 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2005-0146

Description

Firefox before 1.0 and Mozilla before 1.7.5 allow remote attackers to obtain sensitive data from the clipboard via Javascript that generates a middle-click event on systems for which a middle-click performs a paste operation.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0146

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-pfw3-m738-qjww	Firefox before 1.0 and Mozilla before 1.7.5 allow remote attackers to obtain sensitive data from the clipboard via Javascript that generates a middle-click event on systems for which a middle-click performs a paste operation.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.25 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 34.24 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0144

Description

Firefox before 1.0 and Mozilla before 1.7.5 display the secure site lock icon when a view-source: URL references a secure SSL site while an insecure page is being loaded, which could facilitate phishing attacks.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0144

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-gj3c-pxvc-4hrg	Firefox before 1.0 and Mozilla before 1.7.5 display the secure site lock icon when a view-source: URL references a secure SSL site while an insecure page is being loaded, which could facilitate phishing attacks.	2022-05-01	2022-05-01

Assessment

Summary



CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.13 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 51.15 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0143

Description

Firefox before 1.0 and Mozilla before 1.7.5 display the SSL lock icon when an insecure page loads a binary file from a trusted site, which could facilitate phishing attacks.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0143

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-8f62-jh9f-ffg5	Firefox before 1.0 and Mozilla before 1.7.5 display the SSL lock icon when an insecure page loads a binary file from a trusted site, which could facilitate phishing attacks.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Low
---------------	---------	-----

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.18 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 43.62 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0142

Description

Firefox 0.9, Thunderbird 0.6 and other versions before 0.9, and Mozilla 1.7 before 1.7.5 save temporary files with world-readable permissions, which allows local users to read certain web content or attachments that belong to other users, e.g. content that is managed by helper applications such as PDF.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0142

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.1	AV:L/AC:L/Au:N/C:P/I:N/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-q449-wmj9-fjj4	Firefox 0.9, Thunderbird 0.6 and other versions before 0.9, and Mozilla 1.7 before 1.7.5 save temporary files with world-readable permissions, which allows local users to read certain web content or attachments that belong to other users, e.g. content that is managed by helper applications such as PDF.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Low
Insignificant	Default	Low

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:P/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2005-0141

Description

Firefox before 1.0 and Mozilla before 1.7.5 allow remote attackers to load local files via links "with a custom getter and toString method" that are middle-clicked by the user to be opened in a new tab.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0141

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:P/I:N/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-jj36-3392-jhm7	Firefox before 1.0 and Mozilla before 1.7.5 allow remote attackers to load local files via links "with a custom getter and toString method" that are middle-clicked by the user to be opened in a new tab.	2022-05-01	2022-05-01

Assessment

Summary

Insignificant	Default	Low

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:P/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.18 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 43.36 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-1614

Description

Mozilla allows remote attackers to cause a denial of service (application crash from invalid memory access) via an "unusual combination of visual elements," including several large MARQUEE tags with large height parameters, as demonstrated by mangleme.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-1614

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-cfrm-mc6g-2q3f	Mozilla allows remote attackers to cause a denial of service (application crash from invalid memory access) via an "unusual combination of visual elements," including several large MARQUEE tags with large height parameters, as demonstrated by mangleme.	2022-04-29	2022-04-29

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.34 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 13.35 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Mozilla allows remote attackers to cause a denial of service (application crash from null dereference or infinite loop) via a web page that contains a (1) TEXTAREA, (2) INPUT, (3) FRAMESET or (4) IMG tag followed by a null character and some trailing characters, as demonstrated by mangleme.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-1613

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-pqwg-424h- mwmq	Mozilla allows remote attackers to cause a denial of service (application crash from null dereference or infinite loop) via a web page that contains a (1) TEXTAREA, (2) INPUT, (3) FRAMESET or (4) IMG tag followed by a null character and some trailing characters, as demonstrated by mangleme.	2022-04-29	2022-04-29

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi}
Page 191 of 290 Doc. Date: \${document.date_

Criteria	Explanation
EPSS	This vulnerability has a 1.06 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 15.32 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Unknown vulnerability in LiveConnect in Mozilla 1.7 beta allows remote attackers to read arbitrary files in known locations.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-1450

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-9hj8-rmm5-7rx3	Unknown vulnerability in LiveConnect in Mozilla 1.7 beta allows remote attackers to read arbitrary files in known locations.	2022-04-29	2022-04-29

Assessment

Summary



CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versi}Page 192 of 290Doc. Date: \${document.date_

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.21 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 40.10 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Firefox before 1.0 and Mozilla before 1.7.5 allow inactive (background) tabs to focus on input being entered in the active tab, as originally reported using form fields, which allows remote attackers to steal sensitive data that is intended for other sites, which could facilitate phishing attacks.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-1381

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-hhqx-qfww-wwhc	Firefox before 1.0 and Mozilla before 1.7.5 allow inactive (background) tabs to focus on input being entered in the active tab, as originally reported using form fields, which allows remote attackers to steal sensitive data that is intended for other sites, which could facilitate phishing attacks.	2022-04-29	2022-04-29

Assessment

Summary

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

CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi} Page 193 of 290 Doc. Date: \${document.date_

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 16.69 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 3.81 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-1380

Description

Firefox before 1.0 and Mozilla before 1.7.5 allows inactive (background) tabs to launch dialog boxes, which can allow remote attackers to spoof the dialog boxes from web sites in other windows and facilitate phishing attacks, aka the "Dialog Box Spoofing Vulnerability."

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-1380

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-vv9m-2w98-m7rf	Firefox before 1.0 and Mozilla before 1.7.5 allows inactive (background) tabs to launch dialog boxes, which can allow remote attackers to spoof the dialog boxes from web sites in other windows and facilitate phishing attacks, aka the "Dialog Box Spoofing Vulnerability."	2022-04-29	2022-04-29

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.20 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 41.12 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-1316

Description

Heap-based buffer overflow in MSG_UnEscapeSearchUrl in nsNNTPProtocol.cpp for Mozilla 1.7.3 and earlier allows remote attackers to cause a denial of service (application crash) via an NNTP URL (news:) with a trailing '\' (backslash) character, which prevents a string from being NULL terminated.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-1316

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-9c99-v6fv-f744	Heap-based buffer overflow in MSG_UnEscapeSearchUrl in nsNNTPProtocol.cpp for Mozilla 1.7.3 and earlier allows remote attackers to cause a denial of service (application crash) via an NNTP URL (news:) with a trailing '\' (backslash) character, which prevents a string from being NULL terminated.	2022-04-29	2022-04-29

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

	······································
Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 5.84 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 6.35 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-1156

Description

Mozilla before 1.7.6, and Firefox before 1.0.1, allows remote attackers to spoof arbitrary web sites by injecting content from one window into a target window whose name is known but resides in a different domain, as demonstrated using a pop-up window on a trusted web site, aka the "window injection" vulnerability.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-1156

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versi}Page 196 of 290Doc. Date: \${document.date_

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-g6f4-4jhr-qjg5	Mozilla before 1.7.6, and Firefox before 1.0.1, allows remote attackers to spoof arbitrary web sites by injecting content from one window into a target window whose name is known but resides in a different domain, as demonstrated using a pop-up window on a trusted web site, aka the "window injection" vulnerability.	2022-04-29	2022-04-29

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: aV:N/AC:M/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.46 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 24.02 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0909

Description

Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 may allow remote attackers to trick users into performing unexpected actions, including installing software, via signed scripts that request enhanced abilities using the enablePrivilege parameter, then modify the meaning of certain security-relevant dialog messages.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0909

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.1	AV:N/AC:H/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-fmr4-hv22-46fr	Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 may allow remote attackers to trick users into performing unexpected actions, including installing software, via signed scripts that request enhanced abilities using the enablePrivilege parameter, then modify the meaning of certain security-relevant dialog messages.	2022-04-29	2022-04-29

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.89 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 11.05 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows untrusted Javascript code to read and write to the clipboard, and possibly obtain sensitive information, via script-generated events such as Ctrl-Ins.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0908

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-8c73-9gh8-7c8v	Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows untrusted Javascript code to read and write to the clipboard, and possibly obtain sensitive information, via script-generated events such as Ctrl-Ins.	2022-04-29	2022-04-29

Assessment

Summary

Insignificant	Default	Medium
morgimiount	Doradit	Mediam

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:P/I:P/A:N
Keywords	No keyword sets matched.

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi}
Page 199 of 290 Doc. Date: \${document.date_

Criteria	Explanation
EPSS	This vulnerability has a 0.29 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 30.12 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

Description

The Linux install .tar.gz archives for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8, create certain files with insecure permissions, which could allow local users to overwrite those files and execute arbitrary code.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0907

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-jgmj-mpcg-qp5x	The Linux install .tar.gz archives for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8, create certain files with insecure permissions, which could allow local users to overwrite those files and execute arbitrary code.	2022-04-29	2022-04-29

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Doc. Identifier: \${document.id}

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 94.89 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0906

Description

The XPInstall installer in Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 sets insecure permissions for certain installed files within xpi packages, which could allow local users to overwrite arbitrary files or execute arbitrary code.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0906

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-2vph-3h86-9f5r	The XPInstall installer in Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 sets insecure permissions for certain installed files within xpi packages, which could allow local users to overwrite arbitrary files or execute arbitrary code.	2022-04-29	2022-04-29

Assessment

Summary

Insignificant	Default	Medium
insignincant	Delault	Wedium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.09 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 61.70 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0905

Description

Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows remote attackers to perform cross-domain scripting and possibly execute arbitrary code by convincing a user to drag and drop javascript: links to a frame or page in another domain.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0905

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-fqjg-fc86-m5cr	Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows remote attackers to perform cross-domain scripting and possibly execute arbitrary code by convincing a user to drag and drop javascript: links to a frame or page in another domain.	2022-04-29	2022-04-29

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:L/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.13 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 10.38 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0904

Description

Integer overflow in the bitmap (BMP) decoder for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allow remote attackers to execute arbitrary code via wide bitmap files that trigger heap-based buffer overflows.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0904

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-238r-rqpq-9cqf	Integer overflow in the bitmap (BMP) decoder for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allow remote attackers to execute arbitrary code via wide bitmap files that trigger heap-based buffer overflows.	2022-04-29	2022-04-29

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

• •			
Criteria	Explanation		
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C		
Keywords	No keyword sets matched.		
EPSS	This vulnerability has a 13.30 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 4.24 % of all scored vulnerabilities.		
KEV	This vulnerability has not been confirmed to have been exploited in the wild.		
EOL	No end-of-life (EOL) information available.		
Assessment	The vulnerability status is in review .		

CVE-2004-0903

Description

Stack-based buffer overflow in the writeGroup function in nsVCardObj.cpp for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows remote attackers to execute arbitrary code via malformed VCard attachments that are not properly handled when previewing a message.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0903

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-q3j6-xfjj-26q5	Stack-based buffer overflow in the writeGroup function in nsVCardObj.cpp for Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allows remote attackers to execute arbitrary code via malformed VCard attachments that are not properly handled when previewing a message.	2022-04-29	2022-04-29

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 13.25 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 4.25 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2004-0902

Description

Multiple heap-based buffer overflows in Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allow remote attackers to cause a denial of service (application crash) or execute arbitrary code via (1) the "Send page" functionality, (2) certain responses from a malicious POP3 server, or (3) a link containing a non-ASCII hostname.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0902

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-53rc-xfx7-6qmc	Multiple heap-based buffer overflows in Mozilla Firefox before the Preview Release, Mozilla before 1.7.3, and Thunderbird before 0.8 allow remote attackers to cause a denial of service (application crash) or execute arbitrary code via (1) the "Send page" functionality, (2) certain responses from a malicious POP3 server, or (3) a link containing a non-ASCII hostname.	2022-04-29	2022-04-29

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (10.7 from base score 10.0)

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 56.04 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 2.22 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

The cert_TestHostName function in Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, only checks the hostname portion of a certificate when the hostname portion of the URI is not a fully qualified domain name (FQDN), which allows remote attackers to spoof trusted certificates.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0765

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

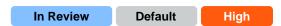
Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-h29q-7v28-gprh	The cert_TestHostName function in Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, only checks the hostname portion of a certificate when the hostname portion of the URI is not a fully qualified domain name (FQDN), which allows remote attackers to spoof trusted certificates.	2022-04-29	2022-04-29

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.

Doc. Identifier: \${document.id}

\${document.name} Page 207 of 290 Doc. Version: \${document.versic Doc. Date: \${document.date_

Criteria	Explanation
EPSS	This vulnerability has a 0.38 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 26.14 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote web sites to hijack the user interface via the "chrome" flag and XML User Interface Language (XUL) files.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0764

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-pw9h-wwm9- 4h36	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote web sites to hijack the user interface via the "chrome" flag and XML User Interface Language (XUL) files.	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.96 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 10.81 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2004-0762

Description

Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote web sites to install arbitrary extensions by using interactive events to manipulate the XPInstall Security dialog box.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0762

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-254j-3m2w-23xr	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote web sites to install arbitrary extensions by using interactive events to manipulate the XPInstall Security dialog box.	2022-05-03	2022-05-03

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.06 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 15.24 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0761

Description

Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote attackers to use certain redirect sequences to spoof the security lock icon that makes a web page appear to be encrypted.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0761

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-v4fj-43xc-9937	Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, allow remote attackers to use certain redirect sequences to spoof the security lock icon that makes a web page appear to be encrypted.	2022-05-03	2022-05-03

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versi}Page 210 of 290Doc. Date: \${document.date_

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.56 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 21.72 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0760

Description

Mozilla allows remote attackers to cause Mozilla to open a URI as a different MIME type than expected via a null character (%00) in an FTP URI.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0760

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-75wj-j7cg-5q44	Mozilla allows remote attackers to cause Mozilla to open a URI as a different MIME type than expected via a null character (%00) in an FTP URI.	2022-05-03	2022-05-03

Assessment

Summary

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

	·
Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.51 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 12.53 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0759

Description

Mozilla before 1.7 allows remote web servers to read arbitrary files via Javascript that sets the value of an <input type="file"> tag.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0759

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-q2hq-vr9g-6x97	Mozilla before 1.7 allows remote web servers to read arbitrary files via Javascript that sets the value of an <input type="file"/> tag.	2022-05-03	2022-05-03

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.62 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 20.56 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0758

Description

Mozilla 1.5 through 1.7 allows a CA certificate to be imported even when their DN is the same as that of the built-in CA root certificate, which allows remote attackers to cause a denial of service to SSL pages because the malicious certificate is treated as invalid.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0758

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-6ccr-h2cv-pc67	Mozilla 1.5 through 1.7 allows a CA certificate to be imported even when their DN is the same as that of the built-in CA root certificate, which allows remote attackers to cause a denial of service to SSL pages because the malicious certificate is treated as invalid.	2022-05-03	2022-05-03

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 22.66 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 3.32 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2004-0757

Description

Heap-based buffer overflow in the SendUidl in the POP3 capability for Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, may allow remote POP3 mail servers to execute arbitrary code.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0757

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	10.0	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-ffvj-mxf9-q65v	Heap-based buffer overflow in the SendUidl in the POP3 capability for Mozilla before 1.7, Firefox before 0.9, and Thunderbird before 0.7, may allow remote POP3 mail servers to execute arbitrary code.	2022-05-03	2022-05-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.67 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 11.85 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Description

Unknown versions of Mozilla allow remote attackers to cause a denial of service (high CPU/RAM consumption) using Javascript with an infinite loop that continues to add input to a form, possibly as the result of inserting control characters, as demonstrated using an embedded ctrl-U.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0478

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Weakness

CWE-399

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	2.6	AV:N/AC:H/Au:N/C:N/I:N/A:P	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-5435-hp8c-m4q9	Unknown versions of Mozilla allow remote attackers to cause a denial of service (high CPU/RAM consumption) using Javascript with an infinite loop that continues to add input to a form, possibly as the result of inserting control characters, as demonstrated using an embedded ctrl-U.	2022-04-29	2022-04-29

Assessment

Summary

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:H/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.75 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 18.47 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2002-2364

Description

Cross-site scripting (XSS) vulnerability in PHP Ticket 0.5 and earlier allows remote attackers to inject arbitrary web script or HTML via a help ticket.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2002-2364

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-79

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-cxx3-573v-vcgm	Cross-site scripting (XSS) vulnerability in PHP Ticket 0.5 and earlier allows remote attackers to inject arbitrary web script or HTML via a help ticket.	2022-04-30	2022-04-30

Assessment

Summary

Insignificant	Default	Medium

Doc. Identifier: \${document.id} \${document.name} Doc. Version: \${document.versions page 217 of 290 Doc. Date: \${document.date_}}

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.14 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 48.52 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2002-2362

Description

Cross-site scripting (XSS) vulnerability in form_header.php in MyMarket 1.71 allows remote attackers to inject arbitrary web script or HTML via the noticemsg parameter.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2002-2362

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Weakness

CWE-79

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-rhp6-27r4-xwgx	Cross-site scripting (XSS) vulnerability in form_header.php in MyMarket 1.71 allows remote attackers to inject arbitrary web script or HTML via the noticemsg parameter.	2022-04-30	2022-04-30

Doc. Identifier: \${document.id}\${document.name}Doc. Version: \${document.versi}Page 218 of 290Doc. Date: \${document.date_

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:M/Au:N/C:N/I:P/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.25 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 34.61 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2002-0815

Description

The Javascript "Same Origin Policy" (SOP), as implemented in (1) Netscape, (2) Mozilla, and (3) Internet Explorer, allows a remote web server to access HTTP and SOAP/XML content from restricted sites by mapping the malicious server's parent DNS domain name to the restricted site, loading a page from the restricted site into one frame, and passing the information to the attacker-controlled frame, which is allowed because the document.domain of the two frames matches on the parent domain.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2002-0815

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-6p7q-r2p3-gx4g	The Javascript "Same Origin Policy" (SOP), as implemented in (1) Netscape, (2) Mozilla, and (3) Internet Explorer, allows a remote web server to access HTTP and SOAP/XML content from restricted sites by mapping the malicious server's parent DNS domain name to the restricted site, loading a page from the restricted site into one frame, and passing the information to the attacker-controlled frame, which is allowed because the document.domain of the two frames matches on the parent domain.	2022-04-30	2022-04-30

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.30 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 29.75 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2001-0234

Description

NewsDaemon before 0.21b allows remote attackers to execute arbitrary SQL queries and gain privileges via a malformed user_username parameter.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2001-0234

Affected Components

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-9xw2-c3qj-x8m5	NewsDaemon before 0.21b allows remote attackers to execute arbitrary SQL queries and gain privileges via a malformed user_username parameter.	2022-04-30	2022-04-30

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.81 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 17.63 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2000-0655

Doc. Identifier: \${document.id}

Description

Netscape Communicator 4.73 and earlier allows remote attackers to cause a denial of service or execute arbitrary commands via a JPEG image containing a comment with an illegal field length of 1.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2000-0655

Affected Components

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-5cwq-wmjx-47pq	Netscape Communicator 4.73 and earlier allows remote attackers to cause a denial of service or execute arbitrary commands via a JPEG image containing a comment with an illegal field length of 1.	2022-05-03	2022-05-03

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.35 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 13.33 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-1999-0377

Description

Process table attack in Unix systems allows a remote attacker to perform a denial of service by filling a machine's process tables through multiple connections to network services.

\${document.classification_en}

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-1999-0377

Affected Components

Component	Artifact Id	Version
Netty/Transport/Native/Unix/Common	netty-transport-native-unix-common-4.1.110.Final.	4.1.110.Final

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	5.0	AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-w9p9-j3v6-q4vf	Process table attack in Unix systems allows a remote attacker to perform a denial of service by filling a machine's process tables through multiple connections to network services.	2022-04-30	2022-04-30

Assessment

Summary

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:2.0 NVD-CNA-NVD provides the vector: AV:N/AC:L/Au:N/C:N/I:N/A:P
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.27 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 31.36 % of all scored vulnerabilities.

Doc. Identifier: \${document.id}

\${document.name} Page 223 of 290 Doc. Version: \${document.versi}
Doc. Date: \${document.date_

Criteria	Explanation
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

4 ae-artifact-analysis Affected Components

juniversalchardet

Artifacts

Component	Artifact Id	Version
juniversalchardet	juniversalchardet-2.4.0.jar	2.4.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-10519	8.8		High		Default	In Review	
	GHSA-gcp3-gfr7-i	rcqp					
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.20.24)				
CVE-2020-10518	8.8		High		Default	In Review	
	GHSA-m5vm-44r4	1-56mf					
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.19.21)				
CVE-2020-10517	4.3		Medium		Default	Insignificant	
	GHSA-38rx-7wc7	-6jvw					
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.19.21)				
CVE-2012-2055	7.5		High		Default	In Review	
	GHSA-8qp2-79w8-8586						
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)						

Table 1: juniversalchardet Vulnerabilities

Caffeine cache

Doc. Identifier: \${document.id}

Artifacts

Component	Artifact Id	Version
Caffeine cache	caffeine-3.1.8.jar	3.1.8

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2012-2055	7.5		High		Default	In Review
	GHSA-8qp2-79w8-8586 cpe:/a:github:github:::~~enterprise~~~ [, 20120304)					

Table 2: Caffeine cache Vulnerabilities

uri-template

Artifacts

Component	Artifact Id	Version
uri-template	uri-template-0.10.jar	0.10

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-10519	8.8		High		Default	In Review	
	GHSA-gcp3-gfr7-i	rcqp					
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.20.24)				
CVE-2020-10518	8.8		High		Default	In Review	
	GHSA-m5vm-44r4	1-56mf					
	cpe:/a:github:githu	ub:::~~enterprise~~	-~ [, 2.19.21)				
CVE-2020-10517	4.3		Medium		Default	Insignificant	
	GHSA-38rx-7wc7-	-6jvw					
	cpe:/a:github:githu	ub:::~~enterprise~~	-~ [, 2.19.21)				
CVE-2012-2055	7.5		High		Default	In Review	
	GHSA-8qp2-79w8-8586						
	cpe:/a:github:githu	ub:::~~enterprise~~	-~ [, 20120304)				

Table 3: uri-template Vulnerabilities

jackson-coreutils-equivalence

Artifacts

Component	Artifact Id	Version
jackson-coreutils-equivalence	jackson-coreutils-equivalence-1.0.jar	1.0

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-10519	8.8		High		Default	In Review
	GHSA-gcp3-gfr7-i	rcqp				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.20.24)			
CVE-2020-10518	10518 8.8 High				Default	In Review
	GHSA-m5vm-44r4	1-56mf				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.19.21)			
CVE-2020-10517	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7	-6jvw				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.19.21)			
CVE-2012-2055	7.5		High		Default	In Review
	GHSA-8qp2-79w8	3-8586				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 20120304)			

Table 4: jackson-coreutils-equivalence Vulnerabilities

msg-simple

Artifacts

Component	Artifact Id	Version
msg-simple	msg-simple-1.2.jar	1.2

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-10519	8.8		High		Default	In Review	
	GHSA-gcp3-gfr7-rcqp						
	cpe:/a:github:githu	ub:::~~enterprise~~	~ [, 2.20.24)				
CVE-2020-10518	8.8		High		Default	In Review	
	GHSA-m5vm-44r4	4-56mf					
	cpe:/a:github:githu	ub:::~~enterprise~~	~ [, 2.19.21)				
CVE-2020-10517	4.3		Medium		Default	Insignificant	
	GHSA-38rx-7wc7-6jvw						
	cpe:/a:github:githu	ub:::~~enterprise~~	~ [, 2.19.21)				
CVE-2012-2055	7.5		High		Default	In Review	

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
	GHSA-8qp2-79w8-8586						
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)						

Table 5: msg-simple Vulnerabilities

json-schema-core

Artifacts

Component	Artifact Id	Version
json-schema-core	json-schema-core-1.2.14.jar	1.2.14

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-10519	8.8		High		Default	In Review	
	GHSA-gcp3-gfr7-i	rcqp					
	cpe:/a:github:githu	ub:::~~enterprise~~	~ [, 2.20.24)				
CVE-2020-10518	8.8		High		Default	In Review	
	GHSA-m5vm-44r4-56mf						
	cpe:/a:github:githu	ub:::~~enterprise~~	~ [, 2.19.21)				
CVE-2020-10517	4.3		Medium		Default	Insignificant	
	GHSA-38rx-7wc7-6jvw						
	cpe:/a:github:githu	ub:::~~enterprise~~	~ [, 2.19.21)				
CVE-2012-2055	7.5		High		Default	In Review	
	GHSA-8qp2-79w8-8586						
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)						

Table 6: json-schema-core Vulnerabilities

btf

Artifacts

Component	Artifact Id	Version
btf	btf-1.3.jar	1.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-10519	8.8		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
	GHSA-gcp3-gfr7-rcqp						
	cpe:/a:github:githu	ıb:::~~enterprise~~	~ [, 2.20.24)				
CVE-2020-10518	8.8		High		Default	In Review	
	GHSA-m5vm-44r4	1-56mf					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)						
CVE-2020-10517	4.3		Medium		Default	Insignificant	
	GHSA-38rx-7wc7-6jvw						
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)						

Table 7: btf Vulnerabilities

jackson-coreutils

Artifacts

Component	Artifact Id	Version
jackson-coreutils	jackson-coreutils-2.0.jar	2.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-10519	8.8		High		Default	In Review	
	GHSA-gcp3-gfr7-i	rcqp					
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.20.24)				
CVE-2020-10518	8.8		High		Default	In Review	
	GHSA-m5vm-44r4	4-56mf					
	cpe:/a:github:githu	ub:::~~enterprise~~	-~ [, 2.19.21)				
CVE-2020-10517	4.3		Medium		Default	Insignificant	
	GHSA-38rx-7wc7	-6jvw					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)						
CVE-2012-2055	7.5		High		Default	In Review	
	GHSA-8qp2-79w8	3-8586					
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)						

Table 8: jackson-coreutils Vulnerabilities

json-schema-validator

Artifacts

Component	Artifact Id	Version
json-schema-validator	json-schema-validator-2.2.14.jar	2.2.14

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-10519	8.8		High		Default	In Review
	GHSA-gcp3-gfr7-i	rcqp				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.20.24)			
CVE-2020-10518	8.8		High		Default	In Review
	GHSA-m5vm-44r4	4-56mf				
	cpe:/a:github:githu	ub:::~~enterprise~~	-~ [, 2.19.21)			
CVE-2020-10517	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7	-6jvw				
	cpe:/a:github:githu	ub:::~~enterprise~~	-~ [, 2.19.21)			
CVE-2012-2055	7.5		High		Default	In Review
	GHSA-8qp2-79w8	3-8586				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 20120304)			

Table 9: json-schema-validator Vulnerabilities

JSONLD Java :: Core

Artifacts

Component	Artifact Id	Version
JSONLD Java :: Core	jsonld-java-0.13.4.jar	0.13.4

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-10519	8.8		High		Default	In Review	
	GHSA-gcp3-gfr7-rcqp						
	cpe:/a:github:github:::~~enterprise~~~ [, 2.20.24)						
CVE-2020-10518	8.8		High		Default	In Review	
	GHSA-m5vm-44r4-56mf						

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:github:githu	ıb:::~~enterprise~~	~ [, 2.19.21)			
CVE-2020-10517	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7-6jvw					
	cpe:/a:github:githu	ıb:::~~enterprise~~	~ [, 2.19.21)			
CVE-2012-2055	7.5		High		Default	In Review
	GHSA-8qp2-79w8	8-8586				
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)					

Table 10: JSONLD Java :: Core Vulnerabilities

PortEx

Artifacts

Component	Artifact Id	Version
PortEx	portex_2.12-4.0.8.jar	4.0.8

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2012-2055	7.5		High		Default	In Review	
	GHSA-8qp2-79w8-8586						
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)						

Table 11: PortEx Vulnerabilities

zstd-jni

Artifacts

Component	Artifact Id	Version
zstd-jni	zstd-jni-1.5.2-4.jar	1.5.2-4

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-10519	8.8		High		Default	In Review	
	GHSA-gcp3-gfr7-rcqp						
	cpe:/a:github:githu	ıb:::~~enterprise~~	~ [, 2.20.24)				
CVE-2020-10518	8.8		High		Default	In Review	
	GHSA-m5vm-44r4-56mf						

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
	cpe:/a:github:githu	ıb:::~~enterprise~~	~ [, 2.19.21)				
CVE-2020-10517	4.3		Medium		Default	Insignificant	
	GHSA-38rx-7wc7-6jvw						
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)						
CVE-2012-2055	7.5		High		Default	In Review	
	GHSA-8qp2-79w8-8586						
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)						

Table 12: zstd-jni Vulnerabilities

Package URL

Artifacts

Component	Artifact Id	Version
Package URL	packageurl-java-1.5.0.jar	1.5.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-10519	8.8		High		Default	In Review
	GHSA-gcp3-gfr7-i	rcqp				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.20.24)			
CVE-2020-10518	8.8		High		Default	In Review
	GHSA-m5vm-44r4	4-56mf				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.19.21)			
CVE-2020-10517	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7-	-6jvw				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.19.21)			
CVE-2012-2055	7.5		High		Default	In Review
	GHSA-8qp2-79w8	3-8586				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 20120304)			

Table 13: Package URL Vulnerabilities

curvesapi

Artifacts

Component	Artifact Id	Version
curvesapi	curvesapi-1.08.jar	1.08

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-10519	8.8		High		Default	In Review
	GHSA-gcp3-gfr7-i	rcqp				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 2.20.24)			
CVE-2020-10518	8.8		High		Default	In Review
	GHSA-m5vm-44r4	1-56mf				
	cpe:/a:github:githu	ub:::~~enterprise~~	-~ [, 2.19.21)			
CVE-2020-10517	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7	-6jvw				
	cpe:/a:github:githu	ub:::~~enterprise~~	-~ [, 2.19.21)			
CVE-2012-2055	7.5		High		Default	In Review
	GHSA-8qp2-79w8	3-8586				
	cpe:/a:github:githu	ub:::~~enterprise~~	~~ [, 20120304)			

Table 14: curvesapi Vulnerabilities

Guava InternalFutureFailureAccess and InternalFutures

Artifacts

Component	Artifact Id	Version
Guava InternalFutureFailureAccess and InternalFutures	failureaccess-1.0.2.jar	1.0.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2023-2976	7.1		High		Default	In Review
	GHSA-7g45-4rm6	-3mm3				
	cpe:/a:google:gua	va [, 32.0.0)				
CVE-2020-8908	3.3		Low		Default	Insignificant
	GHSA-5mg8-w23	w-74h3				

Doc. Identifier: \${document.id}

\${document.name} Page 232 of 290 Doc. Version: \${document.versi}
Doc. Date: \${document.date_

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:google:guava [, 32.0.0)					

Table 15: Guava InternalFutureFailureAccess and InternalFutures Vulnerabilities

OkHttp

Artifacts

Component	Artifact Id	Version
OkHttp	okhttp-3.14.9.jar	3.14.9

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2023-0833	5.5		Medium		Default	Insignificant
	GHSA-8fhc-q55v-jvx2					
	cpe:/a:squareup:okhttp [, 4.9.2)					

Table 16: OkHttp Vulnerabilities

Okio

Artifacts

Component	Artifact Id	Version
Okio	okio-1.17.2.jar	1.17.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2023-3635	7.5		High		Default	In Review
	GHSA-w33c-445m-f8w7 cpe:/a:squareup:okio [0.5.0, 1.17.6), GHSA com.squareup.okio:okio (Maven) [0, 1.17.6)					

Table 17: Okio Vulnerabilities

Fabric8:: Kubernetes:: Java Client API

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes :: Java Client API	kubernetes-client-api-6.13.3.jar	6.13.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-25738	6.7		Medium		Default	Insignificant
	GHSA-m8wh-mqg	gf-rr8g				
	cpe:/a:kubernetes	:java [, 9.0.2]				
CVE-2020-8570	9.1		Critical		Default	In Review
	GHSA-cghx-9gcr-	r42x				
	cpe:/a:kubernetes	:java [, 9.0.2)				
CVE-2020-8554	5.0		Medium		Default	Insignificant
	GHSA-j9wf-vvm6-	4r9w				
	cpe:/a:kubernetes	:kubernetes				

Table 18: Fabric8:: Kubernetes:: Java Client API Vulnerabilities

Fabric8:: Kubernetes:: HttpClient:: OkHttp

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes :: HttpClient :: OkHttp	kubernetes-httpclient-okhttp-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-8554	5.0		Medium		Default	Insignificant
	GHSA-j9wf-vvm6-	4r9w				
	cpe:/a:kubernetes	:kubernetes				

Table 19: Fabric8 :: Kubernetes :: HttpClient :: OkHttp Vulnerabilities

Fabric8 :: Kubernetes Model :: Admission Registration, Authentication and Authorization

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Admission Registration, Authentication and Authorization	kubernetes-model-admissionregistration-6.13.3.jar	6.13.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-8554	5.0		Medium		Default	Insignificant

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-j9wf-vvm6-4r9w					
	cpe:/a:kubernetes	:kubernetes				

Table 20: Fabric8 :: Kubernetes Model :: Admission Registration, Authentication and Authorization Vulnerabilities

Fabric8:: Kubernetes Model:: API Extensions

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: API Extensions	kubernetes-model-apiextensions-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes	:kubernetes					

Table 21: Fabric8:: Kubernetes Model:: API Extensions Vulnerabilities

Fabric8:: Kubernetes Model:: Apps

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Apps	kubernetes-model-apps-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2020-8554	5.0		Medium		Default	Insignificant		
	GHSA-j9wf-vvm6-4r9w							
	cpe:/a:kubernetes:kubernetes							

Table 22: Fabric8 :: Kubernetes Model :: Apps Vulnerabilities

Fabric8:: Kubernetes Model:: Autoscaling

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Autoscaling	kubernetes-model-autoscaling-6.13.3.jar	6.13.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-8554	5.0		Medium		Default	Insignificant
	GHSA-j9wf-vvm6-	4r9w				
	cpe:/a:kubernetes	:kubernetes				

Table 23: Fabric8 :: Kubernetes Model :: Autoscaling Vulnerabilities

Fabric8:: Kubernetes Model:: Batch

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Batch	kubernetes-model-batch-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes	:kubernetes					

Table 24: Fabric8:: Kubernetes Model:: Batch Vulnerabilities

Fabric8:: Kubernetes Model:: Certificates

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Certificates	kubernetes-model-certificates-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes:kubernetes						

Table 25: Fabric8:: Kubernetes Model:: Certificates Vulnerabilities

Fabric8:: Kubernetes Model:: Common

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Common	kubernetes-model-common-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes	:kubernetes					

Table 26: Fabric8:: Kubernetes Model:: Common Vulnerabilities

Fabric8:: Kubernetes Model:: Coordination

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Coordination	kubernetes-model-coordination-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2020-8554	5.0		Medium		Default	Insignificant		
	GHSA-j9wf-vvm6-4r9w							
	cpe:/a:kubernetes:kubernetes							

Table 27: Fabric8 :: Kubernetes Model :: Coordination Vulnerabilities

Fabric8:: Kubernetes Model:: Core

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Core	kubernetes-model-core-6.13.3.jar	6.13.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-8554	5.0		Medium		Default	Insignificant
	GHSA-j9wf-vvm6-					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
	cpe:/a:kubernetes:kubernetes						

Table 28: Fabric8 :: Kubernetes Model :: Core Vulnerabilities

Fabric8 :: Kubernetes Model :: Discovery

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Discovery	kubernetes-model-discovery-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes:kubernetes						

Table 29: Fabric8 :: Kubernetes Model :: Discovery Vulnerabilities

Fabric8:: Kubernetes Model:: Events

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Events	kubernetes-model-events-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes:kubernetes						

Table 30: Fabric8 :: Kubernetes Model :: Events Vulnerabilities

Fabric8:: Kubernetes Model:: Extensions

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Extensions	kubernetes-model-extensions-6.13.3.jar	6.13.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2020-8554	5.0		Medium		Default	Insignificant		
	GHSA-j9wf-vvm6-4r9w							
	cpe:/a:kubernetes	:kubernetes						

Table 31: Fabric8 :: Kubernetes Model :: Extensions Vulnerabilities

Fabric8:: Kubernetes Model:: FlowControl

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: FlowControl	kubernetes-model-flowcontrol-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes:kubernetes						

Table 32: Fabric8:: Kubernetes Model:: FlowControl Vulnerabilities

Fabric8 :: Kubernetes Model :: Sigs :: Gateway API

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Sigs :: Gateway API	kubernetes-model-gatewayapi-6.13.3.jar	6.13.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes:kubernetes						

Table 33: Fabric8 :: Kubernetes Model :: Sigs :: Gateway API Vulnerabilities

Fabric8:: Kubernetes Model:: Metrics

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Metrics	kubernetes-model-metrics-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-8554	5.0		Medium		Default	Insignificant
	GHSA-j9wf-vvm6-	-4r9w				
	cpe:/a:kubernetes	:kubernetes				

Table 34: Fabric8:: Kubernetes Model:: Metrics Vulnerabilities

Fabric8:: Kubernetes Model:: Networking

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Networking	kubernetes-model-networking-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes:kubernetes						

Table 35: Fabric8:: Kubernetes Model:: Networking Vulnerabilities

Fabric8:: Kubernetes Model:: Node

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Node	kubernetes-model-node-6.13.3.jar	6.13.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-8554	5.0		Medium		Default	Insignificant
	GHSA-j9wf-vvm6-	4r9w				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:kubernetes:kubernetes					

Table 36: Fabric8:: Kubernetes Model:: Node Vulnerabilities

Fabric8 :: Kubernetes Model :: Policy

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Policy	kubernetes-model-policy-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-8554	5.0		Medium		Default	Insignificant
GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes	:kubernetes				

Table 37: Fabric8 :: Kubernetes Model :: Policy Vulnerabilities

Fabric8:: Kubernetes Model:: RBAC

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: RBAC	kubernetes-model-rbac-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes:kubernetes						

Table 38: Fabric8 :: Kubernetes Model :: RBAC Vulnerabilities

Fabric8:: Kubernetes Model:: Resource

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Resource	kubernetes-model-resource-6.13.3.jar	6.13.3

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2020-8554	5.0		Medium		Default	Insignificant	
	GHSA-j9wf-vvm6-4r9w						
	cpe:/a:kubernetes:kubernetes						

Table 39: Fabric8 :: Kubernetes Model :: Resource Vulnerabilities

Fabric8:: Kubernetes Model:: Scheduling

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Scheduling	kubernetes-model-scheduling-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2020-8554	5.0		Medium		Default	Insignificant		
	GHSA-j9wf-vvm6-4r9w							
	cpe:/a:kubernetes:kubernetes							

Table 40: Fabric8 :: Kubernetes Model :: Scheduling Vulnerabilities

Fabric8 :: Kubernetes Model :: Storage Class

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Storage Class	kubernetes-model-storageclass-6.13.3.jar	6.13.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2020-8554	5.0		Medium		Default	Insignificant		
	GHSA-j9wf-vvm6-4r9w							
	cpe:/a:kubernetes:kubernetes							

Table 41: Fabric8 :: Kubernetes Model :: Storage Class Vulnerabilities

io.grpc:grpc-netty

Artifacts

Component	Artifact Id	Version
io.grpc:grpc-netty	grpc-netty-1.69.0.jar	1.69.0

CVE-2023-44487 6.9 Medium Escalate Insignifical CERT-EU-2023-074 GHSA-qppj-fm5r-hxr3 cpe:/a:grpc:grpc:::~~~go~~ [, 1.56.3), cpe:/a:netty:netty [, 4.1.100) CVE-2023-34462 6.5 Medium Default Insignifical GHSA-6mjq-h674-j845 cpe:/a:netty:netty [, 4.1.94) CVE-2022-41881 7.5 High Default In Review GHSA-fx2c-96vj-985v cpe:/a:netty:netty [, 4.1.86) CVE-2022-24823 5.5 Medium Default Insignifical	nt
GHSA-qppj-fm5r-hxr3 cpe:/a:grpc:grpc:::-~~go~~ [, 1.56.3), cpe:/a:netty:netty [, 4.1.100) CVE-2023-34462 6.5 Medium Default Insignification GHSA-6mjq-h674-j845 cpe:/a:netty:netty [, 4.1.94) CVE-2022-41881 7.5 High Default In Review GHSA-fx2c-96vj-985v cpe:/a:netty:netty [, 4.1.86) CVE-2022-24823 5.5 Medium Default Insignification	
cpe:/a:grpc:grpc:::~~~go~~ [, 1.56.3), cpe:/a:netty:netty [, 4.1.100) CVE-2023-34462 6.5 Medium Default Insignifical GHSA-6mjq-h674-j845 cpe:/a:netty:netty [, 4.1.94) CVE-2022-41881 7.5 High Default In Review GHSA-fx2c-96vj-985v cpe:/a:netty:netty [, 4.1.86) CVE-2022-24823 5.5 Medium Default Insignifical	
CVE-2023-34462 6.5 Medium Default Insignification GHSA-6mjq-h674-j845 cpe:/a:netty:netty [, 4.1.94) 7.5 High Default In Review GHSA-fx2c-96vj-985v cpe:/a:netty:netty [, 4.1.86) CVE-2022-24823 5.5 Medium Default Insignification	
GHSA-6mjq-h674-j845 cpe:/a:netty:netty [, 4.1.94) 7.5	
cpe:/a:netty:netty [, 4.1.94) 7.5	
CVE-2022-41881 7.5 High Default In Review GHSA-fx2c-96vj-985v cpe:/a:netty:netty [, 4.1.86) CVE-2022-24823 5.5 Medium Default Insignification	
GHSA-fx2c-96vj-985v cpe:/a:netty:netty [, 4.1.86) CVE-2022-24823 5.5 Medium Default In Review In Review	
cpe:/a:netty:netty [, 4.1.86) CVE-2022-24823 5.5 Medium Default Insignificant	
CVE-2022-24823 5.5 Medium Default Insignification	
Wedium	
	it
GHSA-269q-hmxg-m83q	
cpe:/a:netty:netty [, 4.1.77)	
CVE-2021-43797 6.5 Medium Default Insignification	nt
GHSA-wx5j-54mm-rqqq	
cpe:/a:netty:netty [, 4.1.71)	
CVE-2021-37137 7.5 High Default In Review	
GHSA-9vjp-v76f-g363	
cpe:/a:netty:netty [, 4.1.68)	
CVE-2021-37136 7.5 High Default In Review	
GHSA-grg4-wf29-r9vv	
cpe:/a:netty:netty [, 4.1.68)	
CVE-2021-21409 5.9 Medium Default Insignification	nt
GHSA-f256-j965-7f32	
cpe:/a:netty:netty [, 4.1.61)	



Table 42: io.grpc:grpc-netty Vulnerabilities

Netty/Common

Artifacts

Component	Artifact Id	Version
Netty/Common	netty-common-4.1.110.Final.jar	4.1.110.Final

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2024-47535	7.0		High		Default	In Review	
	GHSA-xq3w-v528-46rv						

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA io.netty:netty-common (Maven) [0, 4.1.115)					

Table 43: Netty/Common Vulnerabilities

Netty/Transport/Native/Unix/Common

Artifacts

Component	Artifact Id	Version
Netty/Transport/Native/Unix/Common	netty-transport-native-unix-common-4.1.110.Final.	4.1.110.Final

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2009-1251	10.0		Critical		Default	In Review
	GHSA-2xj8-3jr2-7qw3					
	cpe:/o:unix:unix					
CVE-1999-0377	5.0		Medium		Default	Insignificant
	GHSA-w9p9-j3v6-	q4vf				
	cpe:/o:unix:unix					

Table 44: Netty/Transport/Native/Unix/Common Vulnerabilities

CDI APIs

Artifacts

Component	Artifact Id	Version
CDI APIs	cdi-api-1.2.jar	1.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2007-1157	7.6		High		Default	In Review
	GHSA-r86m-hxp8-3mvw					
	cpe:/a:jboss:jboss					

Table 45: CDI APIs Vulnerabilities

JTidy

Artifacts

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2023-34623	7.5		High		Default	In Review
	GHSA-fv2r-hw24-	8rxj				
	cpe:/a:jtidy_projec	ct:jtidy [, r938]				
CVE-2008-6161	4.3		Medium		Default	Insignificant
	GHSA-682j-rhpc-p	ohrj				
	cpe:/a:sourceforge	e:wow_raid_mana	ger [, 3.5.0]			
CVE-2008-2503	9.3		Critical		Default	In Review
	GHSA-jxq6-p7m9	-896m				
	cpe:/a:sourceforge	e:emule_x-ray:1.2	1.2 (*)			
CVE-2008-2298	7.5		High		Default	In Review
	GHSA-39wm-cmp	6-6mjc				
	cpe:/a:sourceforge	e:web_slider:0.6 0	.6 (*)			
CVE-2008-0501	5.8		Medium		Default	Insignificant
	GHSA-q7mg-4q42	2-3h 7 f				
	cpe:/a:sourceforge	e:phpmyclub:0.0.1	0.0.1 (*)			
CVE-2007-6640	6.4		Medium		Default	Insignificant
	GHSA-jmrg-23pg-	-v7hm				
	cpe:/a:sourceforge	e:creammonkey:0.	9 0.9 (*), cpe:/a:s	sourceforge:grea	asekit:1.2 1.2 (*)	
CVE-2007-1466	6.8		Medium		Default	Insignificant
	GHSA-mc39-g53r	-8cq4				
	cpe:/a:sourceforge	e:wordperfect_doc	ument_importer-	exporter [, 0.8.8]]	
CVE-2007-1137	5.0		Medium		Default	Insignificant
	GHSA-x927-rp8j-6	62cg				
	cpe:/a:sourceforge	e:putmail:.8 .8 (*)				
CVE-2006-5562	7.5		High		Default	In Review

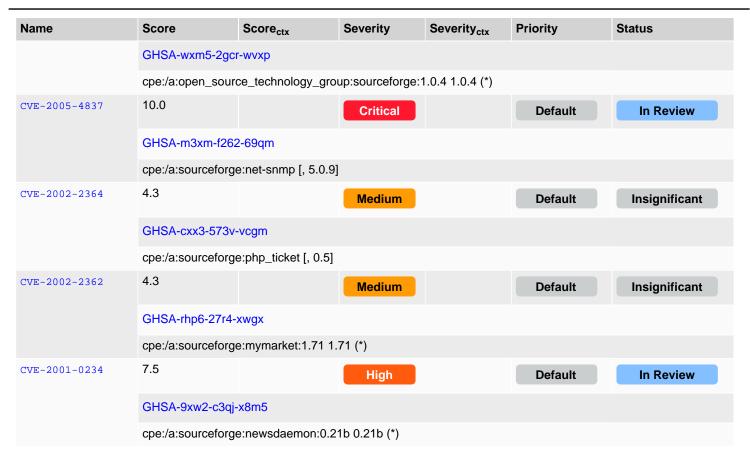


Table 46: JTidy Vulnerabilities

Lucene Common Analyzers

Artifacts

Component	Artifact Id	Version
Lucene Common Analyzers	lucene-analyzers-common-8.11.2.jar	8.11.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-45772	8.0		High		Default	In Review
	GHSA-g643-xq6w-r67c					
	cpe:/a:apache:luc	ene [4.4.0, 9.12.0)				

Table 47: Lucene Common Analyzers Vulnerabilities

Lucene Memory

Artifacts

Component	Artifact Id	Version
Lucene Memory	lucene-backward-codecs-8.11.2.jar	8.11.2

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-45772	8.0		High		Default	In Review
	GHSA-g643-xq6w	∕-r67c				
	cpe:/a:apache:lucene [4.4.0, 9.12.0)					

Table 48: Lucene Memory Vulnerabilities

Lucene Core

Artifacts

Component	Artifact Id	Version
Lucene Core	lucene-core-8.11.2.jar	8.11.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-45772	8.0		High		Default	In Review
	GHSA-g643-xq6w-r67c					
	cpe:/a:apache:lucene [4.4.0, 9.12.0)					

Table 49: Lucene Core Vulnerabilities

Lucene Queries

Artifacts

Component	Artifact Id	Version
Lucene Queries	lucene-queries-8.11.2.jar	8.11.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-45772	8.0		High		Default	In Review
	GHSA-g643-xq6w-r67c					
	cpe:/a:apache:luc	ene [4.4.0, 9.12.0)				

Table 50: Lucene Queries Vulnerabilities

Lucene QueryParsers

Artifacts

Component	Artifact Id	Version
Lucene QueryParsers	lucene-queryparser-8.11.2.jar	8.11.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-45772	8.0		High		Default	In Review
	GHSA-g643-xq6w-r67c					
	cpe:/a:apache:luc	ene [4.4.0, 9.12.0)				

Table 51: Lucene QueryParsers Vulnerabilities

Lucene Sandbox

Artifacts

Component	Artifact Id	Version
Lucene Sandbox	lucene-sandbox-8.11.2.jar	8.11.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-45772	8.0		High		Default	In Review
	GHSA-g643-xq6w-r67c					
	cpe:/a:apache:lucene [4.4.0, 9.12.0)					

Table 52: Lucene Sandbox Vulnerabilities

Doxia :: Core

Artifacts

Component	Artifact Id	Version
Doxia :: Core	doxia-core-1.11.1.jar	1.11.1

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-	9x2x				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					3.1), GHSA org.

Table 53: Doxia :: Core Vulnerabilities

Doxia Sitetools:: Decoration Model

Artifacts

Component	Artifact Id	Version
Doxia Sitetools :: Decoration Model	doxia-decoration-model-1.11.1.jar	1.11.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org apache.maven:maven-core (Maven) [0, 3.8.1)					
						s.1), GHSA org.

Table 54: Doxia Sitetools :: Decoration Model Vulnerabilities

Doxia Sitetools :: Integration Tools

Artifacts

Component	Artifact Id	Version
Doxia Sitetools :: Integration Tools	doxia-integration-tools-1.11.1.jar	1.11.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)					.1), GHSA org.

Table 55: Doxia Sitetools :: Integration Tools Vulnerabilities

Doxia :: Logging API

Artifacts

Component	Artifact Id	Version
Doxia :: Logging API	doxia-logging-api-1.11.1.jar	1.11.1

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 56: Doxia :: Logging API Vulnerabilities

Doxia:: XHTML5 Module

Artifacts

Component	Artifact Id	Version
Doxia :: XHTML5 Module	doxia-module-xhtml5-1.11.1.jar	1.11.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 57: Doxia :: XHTML5 Module Vulnerabilities

Doxia:: XHTML Module

Artifacts

Component	Artifact Id	Version
Doxia :: XHTML Module	doxia-module-xhtml-1.11.1.jar	1.11.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 58: Doxia :: XHTML Module Vulnerabilities

Doxia:: Sink API

Artifacts

Component	Artifact Id	Version
Doxia :: Sink API	doxia-sink-api-1.11.1.jar	1.11.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 59: Doxia :: Sink API Vulnerabilities

Doxia Sitetools:: Site Renderer

Artifacts

Component	Artifact Id	Version
Doxia Sitetools :: Site Renderer	doxia-site-renderer-1.11.1.jar	1.11.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 60: Doxia Sitetools :: Site Renderer Vulnerabilities

Doxia Sitetools :: Skin Model

Artifacts

Component	Artifact Id	Version
Doxia Sitetools :: Skin Model	doxia-skin-model-1.11.1.jar	1.11.1

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 61: Doxia Sitetools :: Skin Model Vulnerabilities

Maven Plugin Tools Java 5 Annotations

Artifacts

Component	Artifact Id	Version
Maven Plugin Tools Java 5 Annotations	maven-plugin-annotations-3.5.jar	3.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 62: Maven Plugin Tools Java 5 Annotations Vulnerabilities

Maven Plugin Tool for Java with Annotations

Artifacts

Component	Artifact Id	Version
Maven Plugin Tool for Java with Annotations	maven-plugin-tools-annotations-3.7.0.jar	3.7.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), apache.maven:maven-core (Maven) [0, 3.8.1)					.1), GHSA org.	

Table 63: Maven Plugin Tool for Java with Annotations Vulnerabilities

Maven Plugin Tools Extractor API

Artifacts

Component	Artifact Id	Version
Maven Plugin Tools Extractor API	maven-plugin-tools-api-3.7.0.jar	3.7.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 64: Maven Plugin Tools Extractor API Vulnerabilities

Maven Plugin Tools Generators

Artifacts

Component	Artifact Id	Version
Maven Plugin Tools Generators	maven-plugin-tools-generators-3.7.0.jar	3.7.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2021-26291	9.1		Critical		Default	In Review		
	GHSA-2f88-5hg8-9x2x							
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)							

Table 65: Maven Plugin Tools Generators Vulnerabilities

Maven Plugin Tool for Java with Javadoc Tags

Artifacts

Component	Artifact Id	Version
Maven Plugin Tool for Java with Javadoc Tags	maven-plugin-tools-java-3.7.0.jar	3.7.0

Vulnerabilities

Doc. Identifier: \${document.id}

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHS apache.maven:maven-core (Maven) [0, 3.8.1)					.1), GHSA org.	

Table 66: Maven Plugin Tool for Java with Javadoc Tags Vulnerabilities

© \${document.copyright.year} \${organization.name}

Maven Plugin Plugin

Artifacts

Component	Artifact Id	Version
Maven Plugin Plugin	maven-plugin-3.7.0.jar	3.7.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 67: Maven Plugin Plugin Vulnerabilities

Apache Maven Reporting API

Artifacts

Component	Artifact Id	Version
Apache Maven Reporting API	maven-reporting-api-3.1.1.jar	3.1.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 68: Apache Maven Reporting API Vulnerabilities

Apache Maven Reporting Implementation

Artifacts

Component	Artifact Id	Version
Apache Maven Reporting Implementation	maven-reporting-impl-3.2.0.jar	3.2.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 69: Apache Maven Reporting Implementation Vulnerabilities

Apache Maven Wagon :: API

Artifacts

Component	Artifact Id	Version
Apache Maven Wagon :: API	wagon-provider-api-2.4.jar	2.4

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 70: Apache Maven Wagon :: API Vulnerabilities

Maven Aether Provider

Artifacts

Component	Artifact Id	Version
Maven Aether Provider	maven-aether-provider-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA apache.maven:maven-core (Maven) [0, 3.8.1)						.1), GHSA org.	

Table 71: Maven Aether Provider Vulnerabilities

Maven Artifact

Artifacts

Component	Artifact Id	Version
Maven Artifact	maven-artifact-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 72: Maven Artifact Vulnerabilities

Maven Compat

Artifacts

Component	Artifact Id	Version
Maven Compat	maven-compat-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					
						3.1), GHSA org.

Table 73: Maven Compat Vulnerabilities

Maven Core

Artifacts

Component	Artifact Id	Version
Maven Core	maven-core-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					.1), GHSA org.

Table 74: Maven Core Vulnerabilities

Doc. Identifier: \${document.id}

Maven Model Builder

Artifacts

Component	Artifact Id	Version
Maven Model Builder	maven-model-builder-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)					.1), GHSA org.

Table 75: Maven Model Builder Vulnerabilities

Maven Model

Artifacts

Component	Artifact Id	Version
Maven Model	maven-model-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					
						8.1), GHSA org.

Table 76: Maven Model Vulnerabilities

Maven Plugin API

Artifacts

Component	Artifact Id	Version
Maven Plugin API	maven-plugin-api-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	· ·	iven [, 3.8.1), GHSA aven-core (Maven)	• .	aven:maven-com	npat (Maven) [0, 3.8	3.1), GHSA org.

Table 77: Maven Plugin API Vulnerabilities

Maven Repository Metadata Model

Artifacts

Component	Artifact Id	Version
Maven Repository Metadata Model	maven-repository-metadata-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 78: Maven Repository Metadata Model Vulnerabilities

Maven Settings Builder

Artifacts

Component	Artifact Id	Version
Maven Settings Builder	maven-settings-builder-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 79: Maven Settings Builder Vulnerabilities

Maven Settings

Artifacts

Component	Artifact Id	Version
Maven Settings	maven-settings-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 80: Maven Settings Vulnerabilities

Apache Thrift

Artifacts

Component	Artifact Id	Version
Apache Thrift	libthrift-0.19.0.jar	0.19.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status			
CVE-2021-24028	9.8		Critical		Default	In Review			
	GHSA-qrr3-c36x-2pcc								
	cpe:/a:facebook:th	nrift [, 2021.02.22.0	00)						
CVE-2019-3565	7.5		High		Default	In Review			
	GHSA-j98f-h9mx-	xrxq							
	cpe:/a:facebook:th	nrift [, 2019.05.06.0	00)						
CVE-2019-3564	7.5		High		Default	In Review			
	GHSA-x4rg-4545-	GHSA-x4rg-4545-4w7w							
	cpe:/a:facebook:th	nrift [, 2019.03.04.0	00)						
CVE-2019-3559	7.5		High		Default	In Review			
	GHSA-6627-jcx5-	j2g8							
	cpe:/a:facebook:th	nrift [, 2019.02.18.0	00)						
CVE-2019-3558	7.5		High		Default	In Review			
	GHSA-7vv7-v9gp	-whmr							
	cpe:/a:facebook:th	nrift [, 2019.02.18.0	00)						
CVE-2019-3553	7.5		High		Default	In Review			
	GHSA-859v-9mcv	/-7rw3							
	cpe:/a:facebook:th	nrift [, 2020.02.03.0	00)						
CVE-2019-3552	7.5		High		Default	In Review			



Table 81: Apache Thrift Vulnerabilities

VelocityTools

Artifacts

Component	Artifact Id	Version
VelocityTools	velocity-tools-2.0.jar	2.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-13959	6.1		Medium		Default	Insignificant
GHSA-fh63-4r66-jc7v						
	cpe:/a:apache:velocity_tools [, 3.1), GHSA org.apache.velocity:velocity-tools (Maven) [0, 2.0]					

Table 82: VelocityTools Vulnerabilities

\${project.groupId}:\${project.artifactId}

Artifacts

Component	Artifact Id	Version
\${project.groupId}:\${project.artifactId}	batik-anim-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-awt-util-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-bridge-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-codec-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-constants-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-css-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-dom-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-ext-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-gvt-1.14.jar	1.14

Doc. Identifier: \${document.id}

\${document.name} Page 261 of 290

Component	Artifact Id	Version
\${project.groupId}:\${project.artifactId}	batik-i18n-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-parser-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-script-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-shared-resources-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-svg-dom-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-svggen-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-transcoder-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-util-1.14.jar	1.14
\${project.groupId}:\${project.artifactId}	batik-xml-1.14.jar	1.14

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2022-44729	7.1		High		Default	In Review		
	GHSA-gq5f-xv48-	2365						
	GHSA org.apache.xmlgraphics:batik-bridge (Maven) [1.0, 1.17), GHSA org.apache.xmlgraphics:batik-transcoder (Maven) [1.0, 1.17)							
CVE-2022-44730	4.4		Medium		Default	Insignificant		
	GHSA-2474-2566-3qxp							
	GHSA org.apache.xmlgraphics:batik-script (Maven) [1.0, 1.17)							

Table 83: \${project.groupId}:\${project.artifactId} Vulnerabilities

Plexus Common Utilities

Artifacts

Component	Artifact Id	Version
Plexus Common Utilities	plexus-utils-2.0.6.jar	2.0.6

Vulnerabilities

Doc. Identifier: \${document.id}

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2022-4245	4.3		Medium		Default	Insignificant
	GHSA-jcwr-x25h-	x5fh				
	cpe:/a:codehaus-p	olexus:plexus-utils	[, 3.0.24), GHSA	org.codehaus.p	lexus:plexus-utils (l	Maven) [0, 3.0.24)
CVE-2022-4244	7.5		High		Default	In Review
	GHSA-g6ph-x5wf	-g337				
	cpe:/a:codehaus-p	olexus:plexus-utils	[, 3.0.24), GHSA	org.codehaus.p	lexus:plexus-utils (l	Maven) [0, 3.0.24)
CVE-2017-1000487	9.8		Critical		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
	GHSA-8vhq-qq4p-grq3 cpe:/a:codehaus-plexus:plexus-utils [, 3.0.16), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.16)						

Table 84: Plexus Common Utilities Vulnerabilities

Plexus Archiver Component

Artifacts

Component	Artifact Id	Version
Plexus Archiver Component	plexus-archiver-4.5.0.jar	4.5.0

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2023-37460	9.8		Critical		Default	In Review	
	GHSA-wh3p-fphp-9h2m						
	cpe:/a:codehaus-plexus:plexus-archiver [, 4.8.0), GHSA org.codehaus.plexus:plexus-archiver (Maven) [0, 4.8.0)						

Table 85: Plexus Archiver Component Vulnerabilities

snappy

Artifacts

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2024-36124	5.3		Medium		Default	Insignificant		
	GHSA-8wh2-6qhj	-h7j9						
	GHSA org.iq80.sr	nappy:snappy (Mav	ren) [0, 0.5)					
CVE-2023-41330	9.8		Critical		Default	In Review		
	GHSA-92rv-4j2h-8	Bmjj						
	cpe:/a:knplabs:snappy [, 1.4.3)							
CVE-2023-28115	9.8		Critical		Default	In Review		
	GHSA-gq6w-q6wh-jggc							
	cpe:/a:knplabs:snappy [, 1.4.2)							

Table 86: snappy Vulnerabilities

Doc. Identifier: \${document.id}

JDOM

Artifacts

Component	Artifact Id	Version
JDOM	jdom2-2.0.6.1.jar	2.0.6.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-33813	7.5		High		Default	In Review
	GHSA-2363-cqg2-863c					
	cpe:/a:jdom:jdom	[, 2.0.6]				

Table 87: JDOM Vulnerabilities

Mozilla Rhino

Artifacts

Component	Artifact Id	Version
Mozilla Rhino	rhino-1.7.7.2.jar	1.7.7.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2009-3014	4.3		Medium		Default	Insignificant
	GHSA-xw9p-2mr3	3-g9mx				
	cpe:/a:mozilla:mo	zilla [, 1.7]				
CVE-2009-3010	4.3		Medium		Default	Insignificant
	GHSA-mv6q-6xw	q-rrw9				
	cpe:/a:mozilla:mo	zilla [, 1.7.12]				
CVE-2007-4039	4.3		Medium		Default	Insignificant
	GHSA-5qrv-2vjc->	wcq				
	cpe:/a:mozilla:mo	zilla				
CVE-2007-1794	10.0		Critical		Default	In Review
	GHSA-whc6-8wvp	o-96v2				
	cpe:/a:mozilla:mo	zilla [, 1.7]				
CVE-2006-6498	6.8		Medium		Due	Insignificant
	GHSA-jmfp-6hwg	-w7qf				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2006-0496	4.3		Medium		Elevated	Insignificant
	GHSA-747m-cwr	6-qmx3				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-4685	6.4		Medium		Default	Insignificant
	GHSA-qx3r-96cr-	cwr5				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-3896	7.8		High		Default	In Review
	GHSA-f389-88pf-	8hp7				
	cpe:/a:mozilla:mo	zilla				
CVE-2005-2270	7.5		High		Default	In Review
	GHSA-jgwp-9p3p	-4h7j				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-2269	7.5		High		Default	In Review
	GHSA-cxw5-72vp	o-8h54				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-2268	2.6		Low		Default	Insignificant
	GHSA-3937-9m8	4-64gp				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-2266	5.0		Medium		Default	Insignificant
	GHSA-gp89-32gv	r-6hww				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-2265	5.0		Medium		Elevated	Insignificant
	GHSA-5pgg-4c5c	-9j5p				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-2263	5.0		Medium		Default	Insignificant
	GHSA-5v66-4mq	r-49xj				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-2261	7.5		High		Default	In Review
	GHSA-j45r-pcwj-8	3g72				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				

\${document.name} Page 265 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2005-2260	7.5		High		Default	In Review
	GHSA-wm6x-mrp	3-f56m				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1937	2.6		Low		Default	Insignificant
	GHSA-ffxc-32xj-v	3rp				
	cpe:/a:mozilla:mo	zilla:1.7.7 1.7.7 (*)				
CVE-2005-1532	7.5		High		Due	In Review
	GHSA-ffv2-fj33-m	vch				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1531	7.5		High		Default	In Review
	GHSA-q7v5-vf67-	fpfr				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1160	5.1		Medium		Default	Insignificant
	GHSA-r5gq-7c27	-jhm8				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1159	7.5		High		Default	In Review
	GHSA-65q8-rprw	-c44f				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1157	7.5		High		Default	In Review
	GHSA-8hfq-wv6x	-73v6				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1156	7.5		High		Default	In Review
	GHSA-p7cq-vpx5	-5pp5				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1155	7.5		High		Escalate	In Review
	GHSA-5f3p-wqh5	-33m5				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1154	7.5		High		Default	In Review
	GHSA-xrcj-fc8v-w	45w				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1153	7.5		High		Default	In Review

\${document.name} Page 266 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-9j3v-w638	-mx3p				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0593	2.6		Low		Default	Insignificant
	GHSA-74mv-jc74	l-mg2v				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0592	7.5		High		Default	In Review
	GHSA-3fwv-8g5j	-79jx				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0590	5.0		Medium		Default	Insignificant
	GHSA-mq4v-fvj7	-qhmj				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0588	5.0		Medium		Default	Insignificant
	GHSA-g63h-wr5d	c-mmgm				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0586	2.6		Low		Default	Insignificant
	GHSA-wrw4-477	q-3qjh				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0585	2.6		Low		Default	Insignificant
	GHSA-cxhx-r8q3	-rf4p				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0584	2.6		Low		Default	Insignificant
	GHSA-v9x2-68hv	v-cwxx				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0578	2.1		Low		Default	Insignificant
	GHSA-7352-x97>	c-grpg				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0401	5.1		Medium		Default	Insignificant
	GHSA-p4xc-fq3x	-cx45				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0399	5.1		Medium		Elevated	Insignificant
	GHSA-x75c-2774	I-mpv3				

\${document.name} Page 267 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0149	5.0		Medium		Default	Insignificant
	GHSA-2x58-77jw	r-wgpw				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0147	7.5		High		Default	In Review
	GHSA-25p3-2r5c	-956q				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0146	5.0		Medium		Default	Insignificant
	GHSA-pfw3-m73	8-qjww				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0144	2.6		Low		Default	Insignificant
	GHSA-gj3c-pxvc-	4hrg				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0143	2.6		Low		Default	Insignificant
	GHSA-8f62-jh9f-f	fg5				
	cpe:/a:mozilla:mo	zilla				
CVE-2005-0142	2.1		Low		Default	Insignificant
	GHSA-q449-wmj	9-fjj4				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0141	2.6		Low		Default	Insignificant
	GHSA-jj36-3392-	jhm7				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2004-1614	5.0		Medium		Default	Insignificant
	GHSA-cfrm-mc6	g-2q3f				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2004-1613	5.0		Medium		Default	Insignificant
	GHSA-pqwg-424	h-mwmq				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2004-1450	5.0		Medium		Default	Insignificant
	GHSA-9hj8-rmm	5-7rx3				
	cpe:/a:mozilla:mo	ozilla:1.7:beta 1.7 (beta)			

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2004-1381	5.0		Medium		Default	Insignificant
	GHSA-hhqx-qfw	w-wwhc				
	cpe:/a:mozilla:m	ozilla				
CVE-2004-1380	5.0		Medium		Default	Insignificant
	GHSA-vv9m-2w	98-m7rf				
	cpe:/a:mozilla:m	ozilla				
CVE-2004-1316	5.0		Medium		Default	Insignificant
	GHSA-9c99-v6f	v-f744				
	cpe:/a:mozilla:m	ozilla				
CVE-2004-1156	4.3		Medium		Default	Insignificant
	GHSA-g6f4-4jhr	-qjg5				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0909	5.1		Medium		Default	Insignificant
	GHSA-fmr4-hv2	2-46fr				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0908	4.0		Medium		Default	Insignificant
	GHSA-8c73-9gh	n8-7c8v				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0907	4.6		Medium		Default	Insignificant
	GHSA-jgmj-mpc	g-qp5x				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0906	4.6		Medium		Default	Insignificant
	GHSA-2vph-3h8	86-9f5r				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0905	4.6		Medium		Default	Insignificant
	GHSA-fqjg-fc86-	-m5cr				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0904	10.0		Critical		Default	In Review
	GHSA-238r-rqpc	q-9cqf				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0903	10.0		Critical		Default	In Review

\${document.name} Page 269 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-q3j6-xfjj-2	26q5				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0902	10.0		Critical		Escalate	In Review
	GHSA-53rc-xfx7	-6qmc				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2004-0765	7.5		High		Default	In Review
	GHSA-h29q-7v2	8-gprh				
	cpe:/a:mozilla:m	ozilla [, 1.7]				
CVE-2004-0764	10.0		Critical		Default	In Review
	GHSA-pw9h-ww	m9-4h36				
	cpe:/a:mozilla:m	ozilla [, 1.7]				
CVE-2004-0762	5.0		Medium		Default	Insignificant
	GHSA-254j-3m2	w-23xr				
	cpe:/a:mozilla:m	ozilla [, 1.7]				
CVE-2004-0761	5.0		Medium		Default	Insignificant
	GHSA-v4fj-43xc	-9937				
	cpe:/a:mozilla:m	ozilla [, 1.7]				
CVE-2004-0760	6.4		Medium		Default	Insignificant
	GHSA-75wj-j7cg	ı-5q44				
	cpe:/a:mozilla:m	ozilla				
CVE-2004-0759	6.4		Medium		Default	Insignificant
	GHSA-q2hq-vr9	g-6x97				
	cpe:/a:mozilla:m	ozilla				
CVE-2004-0758	5.0		Medium		Default	Insignificant
	GHSA-6ccr-h2cv	/-pc67				
	cpe:/a:mozilla:m	ozilla				
CVE-2004-0757	10.0		Critical		Default	In Review
	GHSA-ffvj-mxf9-	q65v				
	cpe:/a:mozilla:m	ozilla [, 1.7]				
CVE-2004-0478	2.6		Low		Default	Insignificant
	GHSA-5435-hp8	c-m4q9				

\${document.name} Page 270 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
	cpe:/a:mozilla:moz	zilla						
CVE-2002-0815	7.5		High		Default	In Review		
	GHSA-6p7q-r2p3-gx4g							
	cpe:/a:mozilla:mozilla							
CVE-2000-0655	5.0		Medium		Default	Insignificant		
	GHSA-5cwq-wmjx	c-47pq						
	cpe:/a:mozilla:moz	zilla:m15 m15 (*)						

Table 88: Mozilla Rhino Vulnerabilities

XZ for Java

Artifacts

Component	Artifact Id	Version
XZ for Java	xz-1.9.jar	1.9

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2022-1271	8.8		High		Default	In Review		
	GHSA-jrpw-543v-	Br62						
	cpe:/a:tukaani:xz	, 5.2.5)						
CVE-2015-4035	7.8		High		Default	In Review		
	GHSA-mf33-8p24-6h53							
	cpe:/a:tukaani:xz::	beta * (beta)[, 4.99	9.9]					

Table 89: XZ for Java Vulnerabilities

Xalan Java Serializer

Artifacts

Component	Artifact Id	Version
Xalan Java Serializer	serializer-2.7.2.jar	2.7.2

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2022-34169	7.5		High		Default	In Review
	GHSA-9339-86wo	:-4qgf				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:apache:xal	an-java [, 2.7.2], Gl	HSA xalan:xalan	(Maven) [0, 2.7	.3)	

Table 90: Xalan Java Serializer Vulnerabilities

5 ae-artifact-analysis Vulnerability Notice

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.

6 ae-artifact-analysis Vulnerability List

The following vulnerabilities have been identified and categorized.

Applicable

No vulnerabilities are considered Applicable within the given configuration.

In Review

The following vulnerabilities are considered In Review within the given configuration:

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2014-8118	10.0		Critical		Default	In Review
	GHSA-wj3v-j872-6	6xqx				
	cpe:/a:rpm:rpm [,	4.12.0]				
CVE-2009-1251	10.0		Critical		Default	In Review
	GHSA-2xj8-3jr2-7	qw3				
	cpe:/o:unix:unix					
CVE-2007-1794	10.0		Critical		Default	In Review
	GHSA-whc6-8wvp	o-96v2				
	cpe:/a:mozilla:moz	zilla [, 1.7]				
CVE-2005-4837	10.0		Critical		Default	In Review
	GHSA-m3xm-f262	2-69qm				
	cpe:/a:sourceforge	e:net-snmp [, 5.0.9]				
CVE-2004-0904	10.0		Critical		Default	In Review
	GHSA-238r-rqpq-	9cqf				
	cpe:/a:mozilla:moz	zilla:1.7 1.7 (*)				
CVE-2004-0903	10.0		Critical		Default	In Review

GHSA-q3[6-xfi]-26q5	Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status				
CVM-2004-0902 10.0 Critical Escalate In Review		GHSA-q3j6-xfjj-2	6q5								
Childa Escalate In Review		cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)								
CVS-2014-0764 10.0	CVE-2004-0902	10.0		Critical		Escalate	In Review				
CVR-2004-0764 10.0 Critical Default In Review		GHSA-53rc-xfx7-	-6qmc								
CHSA-pw9h-wwm9-4h36 cpe/a:mozilla:mozilla [, 1.7] 10.0 Critical Default In Review		cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)								
CV2-2004-0757 10.0 Critical Default In Review	CVE-2004-0764	10.0		Critical		Default	In Review				
CVE-2004-0757		GHSA-pw9h-wwi	m9-4h36								
CVE-2023-41330 9.8 Critical Default In Review		cpe:/a:mozilla:mo	ozilla [, 1.7]								
CVE-2023-41330 9.8 Critical Default In Review	CVE-2004-0757	10.0		Critical		Default	In Review				
Section CVR-2023-41330 9.8 Critical Default In Review		GHSA-ffvj-mxf9-o	q65v								
Critical Default In Review		cpe:/a:mozilla:mo	ozilla [, 1.7]								
CVE-2023-37460 9.8 Critical Default In Review GHSA-wh3p-fphp-9h2m cpe:/a:codehaus-plexus:plexus-archiver [, 4.8.0), GHSA org.codehaus.plexus:plexus-archiver (Maven) [0, 4.8. 0) CVE-2023-28115 9.8 Critical Default In Review GHSA-gq6w-q6wh-jggc cpe:/a:knplabs:snappy [, 1.4.2) Default In Review CVE-2021-24028 9.8 Critical Default In Review GHSA-qr3-c36x-2pcc cpe:/a:facebook:thrift [, 2021.02.22.00) Default In Review CVE-2020-7768 9.8 Critical Default In Review CVE-2020-10683 9.8 Critical Default In Review GHSA-hw/3-m3p6-hj38 Cpe:/a:dom4j_project.dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) Default In Review CVE-2017-9431 9.8 Critical Default In Review	CVE-2023-41330	9.8		Critical		Default	In Review				
Section Sect		GHSA-92rv-4j2h-	-8mjj								
Critical Default In Review		cpe:/a:knplabs:sr	cpe:/a:knplabs:snappy [, 1.4.3)								
CVE-2023-28115 9.8 Critical Default In Review	CVE-2023-37460	9.8		Critical		Default	In Review				
0) CVE-2023-28115 9.8 Critical Default In Review GHSA-gq6w-q6wh-jggc cpe:/a:knplabs:snappy [, 1.4.2) CVE-2021-24028 9.8 Critical Default In Review GHSA-qrr3-c36x-2pcc cpe:/a:facebook:thrift [, 2021.02.22.00) 9.8 Critical Default In Review GHSA-pp75-xfpw-37g9 cpe:/a:grpc:grpc:::~~~node.js~~ [, 1.1.8) CVE-2020-10683 9.8 Critical Default In Review GHSA-hwj3-m3p6-hj38 cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) CVE-2017-9431 9.8 Critical Default In Review		GHSA-wh3p-fphp	o-9h2m								
Critical Default In Review		•	-plexus:plexus-arch	iver [, 4.8.0), GH	SA org.codeha	us.plexus:plexus-ar	chiver (Maven) [0, 4.8.				
cpe:/a:knplabs:snappy [, 1.4.2) GHSA-qrr3-c36x-2pcc cpe:/a:facebook:thrift [, 2021.02.22.00) CVE-2020-7768 9.8 Critical Default In Review CVE-2020-10683 9.8 Critical Default In Review CVE-2020-10683 9.8 Critical Default In Review CVE-2017-9431 9.8 Critical Default In Review	CVE-2023-28115	9.8		Critical		Default	In Review				
Section Sect		GHSA-gq6w-q6w	/h-jggc								
Critical Default In Review											
cpe:/a:facebook:thrift [, 2021.02.22.00) CVE-2020-7768 9.8 Critical Default In Review GHSA-pp75-xfpw-37g9 cpe:/a:grpc:grpc:::~~~node.js~~ [, 1.1.8) CVE-2020-10683 9.8 Critical Default In Review GHSA-hwj3-m3p6-hj38 cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) CVE-2017-9431 9.8 Critical Default In Review	CVE-2021-24028	9.8		Critical		Default	In Review				
CVE-2020-7768 9.8 Critical Default In Review GHSA-pp75-xfpw-37g9 cpe:/a:grpc:grpc:::~~~node.js~~ [, 1.1.8) CVE-2020-10683 9.8 Critical Default In Review GHSA-hwj3-m3p6-hj38 cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) CVE-2017-9431 9.8 Critical Default In Review		GHSA-qrr3-c36x	-2pcc								
GHSA-pp75-xfpw-37g9 cpe:/a:grpc:grpc:::~~node.js~~ [, 1.1.8) CVE-2020-10683 9.8 Critical Default In Review GHSA-hwj3-m3p6-hj38 cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) CVE-2017-9431 9.8 Critical Default In Review		cpe:/a:facebook:t	thrift [, 2021.02.22.0	00)							
cpe:/a:grpc:grpc:::~~~node.js~~ [, 1.1.8) CVE-2020-10683 9.8 Critical Default In Review GHSA-hwj3-m3p6-hj38 cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) CVE-2017-9431 9.8 Critical Default In Review	CVE-2020-7768	9.8		Critical		Default	In Review				
CVE-2020-10683 9.8 Critical Default In Review GHSA-hwj3-m3p6-hj38 cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) CVE-2017-9431 9.8 Critical Default In Review		GHSA-pp75-xfpw	v-37g9								
GHSA-hwj3-m3p6-hj38 cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) CVE-2017-9431 9.8 Critical Default In Review											
cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3) CVE-2017-9431 9.8 Critical Default In Review	CVE-2020-10683	9.8		Critical		Default	In Review				
CVE-2017-9431 9.8 Critical Default In Review		GHSA-hwj3-m3p	GHSA-hwj3-m3p6-hj38								
Default		cpe:/a:dom4j_pro									
GHSA-6q3h-fg8c-jqrj	CVE-2017-9431	9.8		Critical		Default	In Review				
		GHSA-6q3h-fg8c	:-jqrj								

\${document.name} Page 273 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status				
	cpe:/a:grpc:grpc [,	1.2.2]								
CVE-2017-8359	9.8		Critical		Default	In Review				
	GHSA-j2fw-rfr9-pf	rh								
	cpe:/a:grpc:grpc [,	1.2.1]								
CVE-2017-7861	9.8		Critical		Default	In Review				
	GHSA-wgxc-2fq5-	-r7v3								
	cpe:/a:grpc:grpc [,	1.1.2]								
CVE-2017-7860	9.8		Critical		Default	In Review				
	GHSA-j8v6-6xq3-	6m4f								
	cpe:/a:grpc:grpc [,	1.1.2]								
CVE-2017-1000487	9.8		Critical		Default	In Review				
	GHSA-8vhq-qq4p	-grq3								
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.16), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.16)									
CVE-2011-3378	9.3		Critical		Default	In Review				
	GHSA-34ff-v8wx-	w9f5								
	cpe:/a:rpm:rpm [,	4.9.1.1]								
CVE-2008-2503	9.3		Critical		Default	In Review				
	GHSA-jxq6-p7m9	-896m								
	cpe:/a:sourceforge	e:emule_x-ray:1.2	1.2 (*)							
CVE-2021-26291	9.1		Critical		Default	In Review				
	GHSA-2f88-5hg8-	9x2x								
		ven [, 3.8.1), GHS/ aven-core (Maven)		aven:maven-con	npat (Maven) [0, 3.8	3.1), GHSA org.				
CVE-2020-8570	9.1		Critical		Default	In Review				
	GHSA-cghx-9gcr-	r42x								
	cpe:/a:kubernetes	:java [, 9.0.2)								
CVE-2019-20445	9.1		Critical		Default	In Review				
	GHSA-p2v9-g2qv	-p635								
	cpe:/a:netty:netty	[, 4.1.44)								
CVE-2019-20444	9.1		Critical		Default	In Review				
	GHSA-cqqj-4p63-	rrmm								
	cpe:/a:netty:netty	[, 4.1.44)								

\${document.name} Page 274 of 290

CVE-2020-1371 8.8	Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE 2020 13996 8.8	CVE-2022-1271	8.8		High		Default	In Review
CVR-2020-19936 8.8		GHSA-jrpw-543v-	-8r62				
CVE-2021-0519 S.8		cpe:/a:tukaani:xz	[, 5.2.5)				
GHSA org.apache.velocity.velocity (Maven) [0, 1.7] CVE-2010-10519 8.8 High Default In Review GHSA-gcp3-gfr7-rcqp cpe/a:github:github:::enterprise [. 2.20.24) 8.8 High Default In Review GHSA-m5vrn-44r4-56mf cpe-/a:github.github::enterprise [. 2.19.21) 8.0 High Default In Review GHSA-g643-xq6w-r67c cpe-/a:apache:lucene [4.4.0, 9.12.0) CVE-2017-9530 7.8 High Default In Review GHSA-cx97-5qm7-6wq7 cpe-/a:irfanview:tools [. 4.50] CVE-2017-7501 7.8 High Default In Review GHSA-dxgrx5gv-64gh cpe-/a:rpm:rpm [. 4.13.0.3) CVE-2016-7080 7.8 High Default In Review GHSA-cx97-sqm7-sqm7 cpe-/a:rymware:tools [. 10.0.8] CVE-2016-7079 7.8 High Default In Review GHSA-wxpj-3x4g-grwp cpe-/a:vmware:tools [. 10.0.8] CVE-2015-4035 7.8 High Default In Review GHSA-mxpj-3x4g-grwp cpe-/a:vmware:tools [. 10.0.8] CVE-2015-4035 7.8 High Default In Review GHSA-mid3-8p24-6h53 cpe-/a:tukaanixx::beta * (beta)[. 4.999.9]	CVE-2020-13936	8.8		High		Default	In Review
### CVE-2010-10519 8.8 High		GHSA-59j4-wjwp-	-mw9m				
GHSA-gp3-gfr7-rcqp		GHSA org.apache	e.velocity:velocity ((Maven) [0, 1.7]			
cye-/a:github:github:::enterprise [, 2.20.24) CVE-2020-10518 8.8 High Default In Review GHSA-m5vm-44r4-56mf cpe:/a:github:github::enterprise [, 2.19.21) CVE-2024-45772 8.0 High Default In Review GHSA-g643-xq6w-r67c cpe:/a:apache:lucene [4.4.0, 9.12.0) CVE-2017-9530 7.8 High Default In Review GHSA-cx97-5qm7-6wq7 cpe:/a:irfanview:tools [, 4.50] CVE-2017-7501 7.8 High Default In Review GHSA-3xgr-x5gv-64gh cpe:/a:rpm:rpm [, 4.13.0.3) CVE-2016-7080 7.8 High Default In Review GHSA-cp2g-84gg-w9jr cpe:/a:rymware:tools [, 10.0.8] T.8 High Default In Review GHSA-wpi-3x4g-grwp cpe:/a:rymware:tools [, 10.0.8] T.8 High Default In Review GHSA-mf33-8p24-6h53 cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9] T.8 High Default In Review	CVE-2020-10519	8.8		High		Default	In Review
### CVE-2020-10518 8.8 High Default In Review		GHSA-gcp3-gfr7-	rcqp				
CVE-2024-45772 8.0 High Default In Review		cpe:/a:github:gith	ub:::~~enterprise~	~~ [, 2.20.24)			
cpe//argithub:rgithub:rienterprise [, 2.19.21) CVE-2024-45772 8.0 High Default In Review GHSA-g643-xq6w-r67c cpe//arapache:lucene [4.4.0, 9.12.0) T.8 High Default In Review CVE-2017-9530 7.8 High Default In Review GHSA-cx97-5qm7-6wq7 cpe:/a:irfanview:tools [, 4.50] T.8 High Default In Review GHSA-3xgr-x5gv-64gh cpe:/a:rpm:rpm [, 4.13.0.3) T.8 High Default In Review GHSA-cp2g-849g-w9jr cpe:/a:vmware:tools [, 10.0.8] T.8 High Default In Review GHSA-wxpj-3x4g-grwp cpe:/a:vmware:tools [, 10.0.8] T.8 High Default In Review CVE-2015-4035 7.8 High Default In Review	CVE-2020-10518	8.8		High		Default	In Review
CVE-2014-45772 8.0		GHSA-m5vm-44r	4-56mf				
GHSA-g643-xq6w-r67c cpe:/a:apache:lucene [4.4.0, 9.12.0) 7.8		cpe:/a:github:gith	ub:::~~enterprise~	~~ [, 2.19.21)			
CVE-2017-9530 7.8	CVE-2024-45772	8.0		High		Default	In Review
CVE-2017-9530 7.8		GHSA-g643-xq6v	v-r67c				
GHSA-cx97-5qm7-6wq7 cpe:/a:irfanview:tools [, 4.50] CVE-2017-7501 7.8 High Default In Review GHSA-3xgr-x5gv-64gh cpe:/a:rpm:rpm [, 4.13.0.3) CVE-2016-7080 7.8 High Default In Review GHSA-cp2g-849g-w9jr cpe:/a:vmware:tools [, 10.0.8] CVE-2016-7079 7.8 High Default In Review GHSA-wxpj-3x4g-grwp cpe:/a:vmware:tools [, 10.0.8] CVE-2015-4035 7.8 High Default In Review GHSA-mrf33-8p24-6h53 cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]		cpe:/a:apache:luc	cene [4.4.0, 9.12.0)				
CVE-2017-7501 7.8	CVE-2017-9530	7.8		High		Default	In Review
CVE-2017-7501 7.8 High Default In Review GHSA-3xgr-x5gv-64gh cpe:/a:rpm:rpm [, 4.13.0.3) CVE-2016-7080 7.8 High Default In Review GHSA-cp2g-849g-w9jr cpe:/a:vmware:tools [, 10.0.8] CVE-2016-7079 7.8 High Default In Review GHSA-wxpj-3x4g-grwp cpe:/a:vmware:tools [, 10.0.8] CVE-2015-4035 7.8 High Default In Review GHSA-mf33-8p24-6h53 cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]		GHSA-cx97-5qm	7-6wq7				
GHSA-3xgr-x5gv-64gh cpe:/a:rpm:rpm [, 4.13.0.3) CVE-2016-7080 7.8 High Default In Review GHSA-cp2g-849g-w9jr cpe:/a:vmware:tools [, 10.0.8] CVE-2016-7079 7.8 High Default In Review GHSA-wxpj-3x4g-grwp cpe:/a:vmware:tools [, 10.0.8] CVE-2015-4035 7.8 High Default In Review GHSA-mf33-8p24-6h53 cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]		cpe:/a:irfanview:to	ools [, 4.50]				
CVE-2016-7080 7.8 High Default In Review	CVE-2017-7501	7.8		High		Default	In Review
CVE-2016-7080 7.8 High Default In Review		GHSA-3xgr-x5gv-	-64gh				
GHSA-cp2g-849g-w9jr cpe:/a:vmware:tools [, 10.0.8] CVE-2016-7079 7.8 High Default In Review GHSA-wxpj-3x4g-grwp cpe:/a:vmware:tools [, 10.0.8] CVE-2015-4035 7.8 High Default In Review GHSA-mf33-8p24-6h53 cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]		cpe:/a:rpm:rpm [,	4.13.0.3)				
CVE-2016-7079 7.8 High Default In Review	CVE-2016-7080	7.8		High		Default	In Review
CVE-2016-7079 7.8 High Default In Review GHSA-wxpj-3x4g-grwp cpe:/a:vmware:tools [, 10.0.8] 7.8 High Default In Review GHSA-mf33-8p24-6h53 cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]		GHSA-cp2g-849g	ı-w9jr				
GHSA-wxpj-3x4g-grwp cpe:/a:vmware:tools [, 10.0.8] 7.8		cpe:/a:vmware:to	ols [, 10.0.8]				
cpe:/a:vmware:tools [, 10.0.8] 7.8	CVE-2016-7079	7.8		High		Default	In Review
CVE-2015-4035 7.8 High Default In Review CVE-2015-4035 Cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]		GHSA-wxpj-3x4g	-grwp				
GHSA-mf33-8p24-6h53 cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]		cpe:/a:vmware:to	ols [, 10.0.8]				
cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]	CVE-2015-4035	7.8		High		Default	In Review
70		GHSA-mf33-8p24	1-6h53				
CVE-2005-3896 7.8 High Default In Review		cpe:/a:tukaani:xz:	:beta * (beta)[, 4.9	99.9]			
	CVE-2005-3896	7.8		High		Default	In Review

\${document.name} Page 275 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status			
	GHSA-f389-88pf-	8hp7							
	cpe:/a:mozilla:mo	zilla							
CVE-2013-6435	7.6		High		Default	In Review			
	GHSA-qww5-w98	3g-66q7							
	cpe:/a:rpm:rpm [,	4.11.1]							
CVE-2007-1157	7.6		High		Default	In Review			
	GHSA-r86m-hxp8-3mvw								
	cpe:/a:jboss:jboss	3							
CVE-2023-3635	7.5		High		Default	In Review			
	GHSA-w33c-445	n-f8w7							
	cpe:/a:squareup:	okio [0.5.0, 1.17.6),	GHSA com.squ	areup.okio:okio	(Maven) [0, 1.17.6)				
CVE-2023-34623	7.5		High		Default	In Review			
	GHSA-fv2r-hw24	-8rxj							
	cpe:/a:jtidy_proje	ct:jtidy [, r938]							
CVE-2023-33953	7.5		High		Default	In Review			
	GHSA-496j-2rq6-	j6cc							
	cpe:/a:grpc:grpc::	:~~~~ [, 1.53.2)							
CVE-2022-4244	7.5		High		Default	In Review			
	GHSA-g6ph-x5wl	-g337							
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.24), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.24)								
CVE-2022-41881	7.5		High		Default	In Review			
	GHSA-fx2c-96vj-	985v							
	cpe:/a:netty:netty	[, 4.1.86)							
CVE-2022-34169	7.5		High		Default	In Review			
	GHSA-9339-86w	c-4qgf							
	cpe:/a:apache:xa	cpe:/a:apache:xalan-java [, 2.7.2], GHSA xalan:xalan (Maven) [0, 2.7.3)							
CVE-2021-37137	7.5		High		Default	In Review			
	GHSA-9vjp-v76f-	g363							
	cpe:/a:netty:netty	[, 4.1.68)							
CVE-2021-37136	7.5		High		Default	In Review			
	GHSA-grg4-wf29	-r9vv							

\${document.name} Page 276 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status			
	cpe:/a:netty:netty	[, 4.1.68)							
CVE-2021-33813	7.5		High		Default	In Review			
	GHSA-2363-cqg2	2-863c							
	cpe:/a:jdom:jdom	[, 2.0.6]							
CVE-2019-3565	7.5		High		Default	In Review			
	GHSA-j98f-h9mx-	xrxq							
	cpe:/a:facebook:t	hrift [, 2019.05.06.0	00)						
CVE-2019-3564	7.5		High		Default	In Review			
	GHSA-x4rg-4545	-4w7w							
	cpe:/a:facebook:thrift [, 2019.03.04.00)								
CVE-2019-3559	7.5		High		Default	In Review			
	GHSA-6627-jcx5-	j2g8							
	cpe:/a:facebook:t	hrift [, 2019.02.18.0	00)						
CVE-2019-3558	7.5		High		Default	In Review			
	GHSA-7vv7-v9gp	-whmr							
	cpe:/a:facebook:t	hrift [, 2019.02.18.0	00)						
CVE-2019-3553	7.5		High		Default	In Review			
	GHSA-859v-9mc	/-7rw3							
	cpe:/a:facebook:t	hrift [, 2020.02.03.0	00)						
CVE-2019-3552	7.5		High		Default	In Review			
	GHSA-h27g-g76x	r-xqpw							
	cpe:/a:facebook:t	hrift [, 2019.02.18.0	00)						
CVE-2019-16869	7.5		High		Default	In Review			
	GHSA-p979-4mfv	v-53vg							
	cpe:/a:netty:netty	[, 4.1.42)							
CVE-2019-11939	7.5		High		Default	In Review			
	GHSA-w3r9-r9w7	-8h48							
	cpe:/a:facebook:t	hrift [, 2020.03.16.0	00)						
CVE-2019-11938	7.5		High		Default	In Review			
	GHSA-hr4p-8hm2	2-w85x							
	cpe:/a:facebook:t	hrift [, 2019.12.09.0	00)						

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status			
CVE-2018-1000632	7.5		High		Default	In Review			
	GHSA-6pcc-3rfx-	4gpm							
	GHSA org.dom4j:dom4j (Maven) [0, 2.0.3)								
CVE-2015-2156	7.5		High		Default	In Review			
	GHSA-xfv3-rrfm-f	2rv							
	cpe:/a:netty:netty	[, 3.9.7]							
CVE-2014-0114	7.5		High		Escalate	In Review			
	GHSA-p66x-2cv9	-aa3v							
		mmons_beanutils	[, 1.9.1]						
CVE-2012-2055	7.5		High		Default	In Review			
	01104 0 0 70	0.000	· · · · · ·		Dorault				
	GHSA-8qp2-79w8	ub:::~~enterprise~	[20120204)						
CVE-2008-2298	7.5	ub~~enterprise~							
2000 2250	1.0		High		Default	In Review			
	GHSA-39wm-cmp	o6-6mjc							
		e:web_slider:0.6 0	.6 (*)						
CVE-2006-5562	7.5		High		Default	In Review			
	GHSA-wxm5-2gc	r-wvxp							
	cpe:/a:open_source_technology_group:sourceforge:1.0.4 1.0.4 (*)								
CVE-2006-1547	7.5		High		Escalate	In Review			
	GHSA-7qwv-cwgj	-c8rj							
	cpe:/a:apache:co	mmons_beanutils:	1.7.0 1.7.0 (*)						
CVE-2005-2270	7.5		High		Default	In Review			
	GHSA-jgwp-9p3p	-4h7j							
	cpe:/a:mozilla:mo								
CVE-2005-2269	7.5		High		Default	In Review			
	GHSA-cxw5-72vp	-8h5/							
	cpe:/a:mozilla:mo								
CVE-2005-2261	7.5	Za. 1.7 ()	High		Default	In Review			
			High		Delault	III Keview			
	GHSA-j45r-pcwj-8								
or 0005 00	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)							
CVE-2005-2260	7.5		High		Default	In Review			

\${document.name} Page 278 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-wm6x-mrp	o3-f56m				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-1532	7.5		High		Due	In Review
	GHSA-ffv2-fj33-m	nvch				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-1531	7.5		High		Default	In Review
	GHSA-q7v5-vf67	-fpfr				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-1159	7.5		High		Default	In Review
	GHSA-65q8-rprw	-c44f				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-1157	7.5		High		Default	In Review
	GHSA-8hfq-wv6x	:-73v6				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-1156	7.5		High		Default	In Review
	GHSA-p7cq-vpx5	5-5pp5				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-1155	7.5		High		Escalate	In Review
	GHSA-5f3p-wqh5	5-33m5				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-1154	7.5		High		Default	In Review
	GHSA-xrcj-fc8v-v	v45w				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-1153	7.5		High		Default	In Review
	GHSA-9j3v-w638	-mx3p				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0592	7.5		High		Default	In Review
	GHSA-3fwv-8g5j-	-79jx				
	cpe:/a:mozilla:mo	ozilla:1.7 1.7 (*)				
CVE-2005-0147	7.5		High		Default	In Review
	GHSA-25p3-2r5q	-956q				

\${document.name} Page 279 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status			
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)							
CVE-2004-0765	7.5		High		Default	In Review			
	GHSA-h29q-7v28	-gprh							
	cpe:/a:mozilla:mo	zilla [, 1.7]							
CVE-2002-0815	7.5		High		Default	In Review			
	GHSA-6p7q-r2p3-	-gx4g							
	cpe:/a:mozilla:mo	zilla							
CVE-2001-0234	7.5		High		Default	In Review			
	GHSA-9xw2-c3qj-	-x8m5							
	cpe:/a:sourceforge	e:newsdaemon:0.2	21b 0.21b (*)						
CVE-2019-10086	7.3		High		Default	In Review			
	GHSA-6phf-73q6-	-gh87							
	cpe:/a:apache:commons_beanutils [1.0, 1.9.3], GHSA commons-beanutils:commons-beanutils (Maven) [0, 1. 9.4)								
CVE-2010-2199	7.2		High		Default	In Review			
	GHSA-7v29-vf8p-	2rvp							
	cpe:/a:rpm:rpm [,	4.8.0]							
CVE-2010-2198	7.2		High		Default	In Review			
	GHSA-fw46-vp2w	r-pvxq							
	cpe:/a:rpm:rpm [,	4.8.0]							
CVE-2010-2059	7.2		High		Default	In Review			
	GHSA-f3f6-q22p-	8fh5							
	cpe:/a:rpm:rpm [,	4.4.2.3]							
CVE-2005-4889	7.2		High		Default	In Review			
	GHSA-pfqv-vjx4-p	omxj							
	cpe:/a:rpm:rpm [,	4.4.2.3]							
CVE-2023-2976	7.1		High		Default	In Review			
	GHSA-7g45-4rm6	6-3mm3							
	cpe:/a:google:gua	ıva [, 32.0.0)							
CVE-2022-44729	7.1		High		Default	In Review			
	GHSA-gq5f-xv48-	2365							

Table 91: In Review Category (ae-artifact-analysis)

Not Applicable

No vulnerabilities are considered \mathtt{Not} Applicable within the given configuration.

Insignificant

Doc. Identifier: \${document.id}

The following vulnerabilities are considered Insignificant within the given configuration:

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2023-44487	6.9		Medium		Escalate	Insignificant		
	CERT-EU-2023-0	74						
	GHSA-qppj-fm5r-l	nxr3						
	cpe:/a:grpc:grpc:::~~~go~~ [, 1.56.3), cpe:/a:netty:netty [, 4.1.100)							
CVE-2012-0815	6.8		Medium		Default	Insignificant		
	CERT-EU-2012-0	126						
	GHSA-6grx-55mc	-2wmq						
	cpe:/a:rpm:rpm [,	4.9.1.2]						
CVE-2012-0061	6.8		Medium		Default	Insignificant		
	CERT-EU-2012-0	126						
	GHSA-v3v4-hffr-v	r89						
	cpe:/a:rpm:rpm [, 4.9.1.2]							
CVE-2012-0060	6.8		Medium		Default	Insignificant		

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status				
	CERT-EU-20	12-0126								
	GHSA-j6wj-co	GHSA-j6wj-cqmg-hvcm								
	cpe:/a:rpm:rpi	m [, 4.9.1.2]								
CVE-2007-1466	6.8		Medium		Default	Insignificant				
	GHSA-mc39-	g53r-8cq4								
	cpe:/a:source	forge:wordperfect_	document_importe	-exporter [, 0.8.	8]					
CVE-2006-6498	6.8		Medium		Due	Insignificant				
	GHSA-jmfp-6	hwg-w7qf								
	cpe:/a:mozilla	:mozilla:1.7 1.7 (*)								
CVE-2021-35939	6.7		Medium		Default	Insignificant				
	GHSA-prgv-w	33h-5m73								
	cpe:/a:rpm:rpi	m [, 4.18)								
CVE-2021-35938	6.7		Medium		Default	Insignificant				
	GHSA-83gm-	5269-qr3v								
	cpe:/a:rpm:rpi	m [, 4.18.0)								
CVE-2021-25738	6.7		Medium		Default	Insignificant				
	GHSA-m8wh-	mqgf-rr8g								
	cpe:/a:kubern	etes:java [, 9.0.2]								
CVE-2015-5191	6.7		Medium		Default	Insignificant				
	GHSA-4vr2-3	6wr-v82r								
	cpe:/a:vmwar	e:tools [, 10.0.8]								
CVE-2023-34462	6.5		Medium		Default	Insignificant				
	GHSA-6mjq-h	674-j845								
	cpe:/a:netty:n	etty [, 4.1.94)								
CVE-2021-43797	6.5		Medium		Default	Insignificant				
	GHSA-wx5j-5	4mm-rqqq								
	cpe:/a:netty:n	etty [, 4.1.71)								
CVE-2021-35937	6.4		Medium		Default	Insignificant				
	GHSA-63x9-9)q4w-j636								
	cpe:/a:rpm:rpi	m [, 4.18.0)								
CVE-2007-6640	6.4		Medium		Default	Insignificant				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-jmrg-23p	og-v7hm				
	cpe:/a:sourcefo	rge:creammonkey	v:0.9 0.9 (*), cpe:/a	:sourceforge:gre	easekit:1.2 1.2 (*)	
CVE-2005-4685	6.4		Medium		Default	Insignificant
	GHSA-qx3r-960	or-cwr5				
	cpe:/a:mozilla:r	nozilla:1.7 1.7 (*)				
CVE-2004-0760	6.4		Medium		Default	Insignificant
	GHSA-75wj-j7c	g-5q44				
	cpe:/a:mozilla:r	nozilla				
CVE-2004-0759	6.4		Medium		Default	Insignificant
	GHSA-q2hq-vr	9g-6x97				
	cpe:/a:mozilla:r	nozilla				
CVE-2014-4199	6.3		Medium		Default	Insignificant
	GHSA-v55p-68	fc-xxcv				
	cpe:/a:vmware:	tools				
CVE-2020-13959	6.1		Medium		Default	Insignificant
	GHSA-fh63-4r6	66-jc7v				
	cpe:/a:apache:v	velocity_tools [, 3.	1), GHSA org.apac	he.velocity:velo	city-tools (Maven)	[0, 2.0]
CVE-2021-21409	5.9		Medium		Default	Insignificant
	GHSA-f256-j96	5-7f32				
	cpe:/a:netty:net	ty [, 4.1.61)				
CVE-2021-21295	5.9		Medium		Default	Insignificant
	GHSA-wm47-8	v5p-wjpj				
	cpe:/a:netty:net	ty [, 4.1.60)				
CVE-2010-2197	5.8		Medium		Default	Insignificant
	GHSA-6gj2-w2	3f-chf3				
	cpe:/a:rpm:rpm	[, 4.8.0]				
CVE-2008-0501	5.8		Medium		Default	Insignificant
	GHSA-q7mg-4	q42-3h7f				
	cpe:/a:sourcefo	rge:phpmyclub:0.0	0.1 0.0.1 (*)			
CVE-2023-0833	5.5		Medium		Default	Insignificant
	GHSA-8fhc-q55	5v-jvx2				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:squareup:d	okhttp [, 4.9.2)				
CVE-2022-24823	5.5		Medium		Default	Insignificant
	GHSA-269q-hmx	g-m83q				
	cpe:/a:netty:netty	[, 4.1.77)				
CVE-2021-3421	5.5		Medium		Default	Insignificant
	GHSA-f7ww-c7v4	-g682				
	cpe:/a:rpm:rpm [,	4.16.1.3)				
CVE-2021-21290	5.5		Medium		Default	Insignificant
	GHSA-5mcr-gq6c	:-3hq2				
	cpe:/a:netty:netty	[, 4.1.59)				
CVE-2016-5328	5.5		Medium		Default	Insignificant
	GHSA-4h47-vq45	-ccw2				
	cpe:/a:vmware:too	ols [, 10.0.8]				
CVE-2024-36124	5.3		Medium		Default	Insignificant
	GHSA-8wh2-6qhj	-h7j9				
	GHSA org.iq80.sr	nappy:snappy (Mav	ven) [0, 0.5)			
CVE-2023-32732	5.3		Medium		Default	Insignificant
	GHSA-9hxf-ppjv-v	w6rq				
	cpe:/a:grpc:grpc [, 1.53.0)				
CVE-2021-4277	5.3		Medium		Default	Insignificant
	GHSA-3cqm-26w	8-85g8				
	cpe:/a:utils_projec	ct:utils [, 2021-05-1	4)			
CVE-2005-1160	5.1		Medium		Default	Insignificant
	GHSA-r5gq-7c27	-jhm8				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-0401	5.1		Medium		Default	Insignificant
	GHSA-p4xc-fq3x-	cx45				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-0399	5.1		Medium		Elevated	Insignificant
	GHSA-x75c-2774	-mpv3				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2004-0909	5.1		Medium		Default	Insignificant
	GHSA-fmr4-hv22	2-46fr				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2020-8554	5.0		Medium		Default	Insignificant
	GHSA-j9wf-vvm6	6-4r9w				
	cpe:/a:kubernete	es:kubernetes				
CVE-2014-3488	5.0		Medium		Default	Insignificant
	GHSA-9959-6p3	sm-wxpc				
	cpe:/a:netty:netty					
CVE-2007-1137	5.0		Medium		Default	Insignificant
	GHSA-x927-rp8j	62ca				
		ge:putmail:.8 .8 (*)				
CVE-2005-2266	5.0	ge.putmaiio .o ()	Medium		Default	Insignificant
			Wedium		Delauit	insignincant
	GHSA-gp89-32g					
CVE-2005-2265	cpe:/a:mozilla:me	ozilla:1.7 1.7 (*)				
CVE-2005-2205	3.0		Medium		Elevated	Insignificant
	GHSA-5pgg-4c5	c-9j5p				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2005-2263	5.0		Medium		Default	Insignificant
	GHSA-5v66-4mo	qr-49xj				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2005-0590	5.0		Medium		Default	Insignificant
	GHSA-mq4v-fvj7	'- qhmj				
	cpe:/a:mozilla:m	ozilla:1.7 1.7 (*)				
CVE-2005-0588	5.0		Medium		Default	Insignificant
	GHSA-g63h-wr5	c-mmgm				
	cpe:/a:mozilla:m					
CVE-2005-0149	5.0		Medium		Default	Insignificant
	GHSA-2x58-77jv	v-wgpw				
	cpe:/a:mozilla:m					
	5.0	()	Medium		Default	Insignificant

\${document.name} Page 285 of 290

Name	Score S	core _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-pfw3-m738-q	jww				
	cpe:/a:mozilla:mozill	a:1.7 1.7 (*)				
CVE-2004-1614	5.0		Medium		Default	Insignificant
	GHSA-cfrm-mc6g-2	q3f				
	cpe:/a:mozilla:mozill	a:1.7 1.7 (*)				
CVE-2004-1613	5.0		Medium		Default	Insignificant
	GHSA-pqwg-424h-n	nwmq				
	cpe:/a:mozilla:mozill	a:1.7 1.7 (*)				
CVE-2004-1450	5.0		Medium		Default	Insignificant
	GHSA-9hj8-rmm5-7	rx3				
	cpe:/a:mozilla:mozill	a:1.7:beta 1.7 (b	oeta)			
CVE-2004-1381	5.0		Medium		Default	Insignificant
	GHSA-hhqx-qfww-w	whc				
	cpe:/a:mozilla:mozill	a				
CVE-2004-1380	5.0		Medium		Default	Insignificant
	GHSA-vv9m-2w98-r	n7rf				
	cpe:/a:mozilla:mozill	а				
CVE-2004-1316	5.0		Medium		Default	Insignificant
	GHSA-9c99-v6fv-f74	14				
	cpe:/a:mozilla:mozill	a				
CVE-2004-0762	5.0		Medium		Default	Insignificant
	GHSA-254j-3m2w-2	3xr				
	cpe:/a:mozilla:mozill	a [, 1.7]				
CVE-2004-0761	5.0		Medium		Default	Insignificant
	GHSA-v4fj-43xc-993	37				
	cpe:/a:mozilla:mozill	a [, 1.7]				
CVE-2004-0758	5.0		Medium		Default	Insignificant
	GHSA-6ccr-h2cv-pc	67				
	cpe:/a:mozilla:mozill	a				
CVE-2000-0655	5.0		Medium		Default	Insignificant
	GHSA-5cwq-wmjx-4	7pq				

\${document.name} Page 286 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:mozilla:mo	zilla:m15 m15 (*)				
CVE-1999-0377	5.0		Medium		Default	Insignificant
	GHSA-w9p9-j3v6	-q4vf				
	cpe:/o:unix:unix					
CVE-2021-20266	4.9		Medium		Default	Insignificant
	GHSA-8vf3-43pf-	v3cq				
	cpe:/a:rpm:rpm [,	4.16.1.3)				
CVE-2021-3521	4.7		Medium		Default	Insignificant
	GHSA-pr6x-p264	-jrpq				
	cpe:/a:rpm:rpm [,	4.17.1)				
CVE-2014-4200	4.7		Medium		Default	Insignificant
	GHSA-959q-xww	i-g697				
	cpe:/a:vmware:to	ols				
CVE-2004-0907	4.6		Medium		Default	Insignificant
	GHSA-jgmj-mpcg	-qp5x				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2004-0906	4.6		Medium		Default	Insignificant
	GHSA-2vph-3h86	i-9f5r				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2004-0905	4.6		Medium		Default	Insignificant
	GHSA-fqjg-fc86-n	n5cr				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2022-44730	4.4		Medium		Default	Insignificant
	GHSA-2474-2566	S-3qxp				
	GHSA org.apache	e.xmlgraphics:batik	-script (Maven)	[1.0, 1.17)		
CVE-2022-4245	4.3		Medium		Default	Insignificant
	GHSA-jcwr-x25h-	x5fh				
	cpe:/a:codehaus-	plexus:plexus-utils	[, 3.0.24), GHSA	org.codehaus.	plexus:plexus-utils (Maven) [0, 3.0.24)
CVE-2020-10517	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7	-6jvw				
	cpe:/a:github:gith	ub:::~~enterprise~-	~~ [, 2.19.21)			

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status				
CVE-2009-3014	4.3		Medium		Default	Insignificant				
	GHSA-xw9p-2mr	3-g9mx								
	cpe:/a:mozilla:mo	zilla [, 1.7]								
CVE-2009-3010	4.3		Medium		Default	Insignificant				
	GHSA-mv6q-6xw	q-rrw9								
	cpe:/a:mozilla:mo	cpe:/a:mozilla:mozilla [, 1.7.12]								
CVE-2008-6161	4.3		Medium		Default	Insignificant				
	GHSA-682j-rhpc-	phrj								
	cpe:/a:sourceforg	e:wow_raid_mana	ger [, 3.5.0]							
CVE-2007-4039	4.3		Medium		Default	Insignificant				
	GHSA-5qrv-2vjc-	kwca								
	cpe:/a:mozilla:mo									
CVE-2006-0496	4.3		Medium		Elevated	Insignificant				
	GHSA-747m-cwr	6-amx3								
	cpe:/a:mozilla:mo									
CVE-2004-1156	4.3		Medium		Default	Insignificant				
	GHSA-g6f4-4jhr-c	aig5								
	cpe:/a:mozilla:mo									
CVE-2002-2364	4.3	,	Medium		Default	Insignificant				
	GHSA-cxx3-573v	-veam								
		e:php_ticket [, 0.5]								
CVE-2002-2362	4.3	o.p.:poo. [, o.o]	Medium		Default	Insignificant				
	01104 0 07-4		modium		Doradit	morgimiount				
	GHSA-rhp6-27r4-		74 (*)							
CVE-2004-0908	cpe:/a:sourcerorg	e:mymarket:1.71 1								
CVE 2001 0500	1.0		Medium		Default	Insignificant				
	GHSA-8c73-9gh8									
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)								
CVE-2020-8908	3.3		Low		Default	Insignificant				
	GHSA-5mg8-w23	w-74h3								
	cpe:/a:google:gua	ava [, 32.0.0)								
CVE-2005-2268	2.6		Low		Default	Insignificant				

\${document.name} Page 288 of 290

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-3937-9m84	4-64gp				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-1937	2.6		Low		Default	Insignificant
	GHSA-ffxc-32xj-v	3rp				
	cpe:/a:mozilla:mo	zilla:1.7.7 1.7.7 (*)				
CVE-2005-0593	2.6		Low		Default	Insignificant
	GHSA-74mv-jc74	-mg2v				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-0586	2.6		Low		Default	Insignificant
	GHSA-wrw4-4770	q-3qjh				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-0585	2.6		Low		Default	Insignificant
	GHSA-cxhx-r8q3-	rf4p				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-0584	2.6		Low		Default	Insignificant
	GHSA-v9x2-68hw	/-CWXX				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-0144	2.6		Low		Default	Insignificant
	GHSA-gj3c-pxvc-	4hrg				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2005-0143	2.6		Low		Default	Insignificant
	GHSA-8f62-jh9f-ff	fg5				
	cpe:/a:mozilla:mo	zilla				
CVE-2005-0141	2.6		Low		Default	Insignificant
	GHSA-jj36-3392-j	hm7				
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)				
CVE-2004-0478	2.6		Low		Default	Insignificant
	GHSA-5435-hp8c	-m4q9				
	cpe:/a:mozilla:mo	zilla				
CVE-2005-0578	2.1		Low		Default	Insignificant
	GHSA-7352-x97x	-grpg				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
	cpe:/a:mozilla:mo	zilla:1.7 1.7 (*)					
CVE-2005-0142	2.1		Low		Default	Insignificant	
	GHSA-q449-wmj9-fjj4						
	cpe:/a:mozilla:nozilla:1.7 1.7 (*)						

Table 92: Insignificant Category (ae-artifact-analysis)

Void

No vulnerabilities are considered ${\tt Void}$ within the given configuration.