

\${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.....	8
	CVE-2024-45772.....	10
	CVE-2024-36124.....	11
	CVE-2023-45960.....	12
	CVE-2023-44487.....	13
	CVE-2023-41330.....	14
	CVE-2023-37460.....	16
	CVE-2023-3635.....	17
	CVE-2023-34623.....	18
	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.....	30
	CVE-2022-41881.....	31
	CVE-2022-34169.....	32
	CVE-2022-24823.....	33
	CVE-2022-1271.....	35
	CVE-2021-43797.....	36
	CVE-2021-4277.....	37
	CVE-2021-37137.....	38
	CVE-2021-37136.....	40
	CVE-2021-35939.....	41
	CVE-2021-35938.....	42
	CVE-2021-35937.....	43
	CVE-2021-3521.....	45
	CVE-2021-3421.....	46
	CVE-2021-33813.....	47
	CVE-2021-26291.....	48
	CVE-2021-25738.....	50
	CVE-2021-24028.....	52
	CVE-2021-21409.....	53
	CVE-2021-21295.....	54
	CVE-2021-21290.....	56
	CVE-2021-20266.....	57
	CVE-2020-8908.....	58
	CVE-2020-8570.....	59
	CVE-2020-8554.....	61
	CVE-2020-7768.....	62
	CVE-2020-13959.....	64

CVE-2020-13936.....	65
CVE-2020-10683.....	66
CVE-2020-10519.....	67
CVE-2020-10518.....	69
CVE-2020-10517.....	71
CVE-2019-3565.....	72
CVE-2019-3564.....	74
CVE-2019-3559.....	75
CVE-2019-3558.....	76
CVE-2019-3553.....	77
CVE-2019-3552.....	79
CVE-2019-20445.....	80
CVE-2019-20444.....	81
CVE-2019-16869.....	82
CVE-2019-11939.....	83
CVE-2019-11938.....	85
CVE-2019-10086.....	86
CVE-2018-6969.....	87
CVE-2018-1000632.....	88
CVE-2017-9530.....	90
CVE-2017-9431.....	91
CVE-2017-8359.....	92
CVE-2017-7861.....	93
CVE-2017-7860.....	94
CVE-2017-7501.....	96
CVE-2017-1000487.....	97
CVE-2016-7080.....	98
CVE-2016-7079.....	99
CVE-2016-5328.....	100
CVE-2015-5191.....	102
CVE-2015-4035.....	103
CVE-2015-2156.....	104
CVE-2014-8118.....	105
CVE-2014-4200.....	106
CVE-2014-4199.....	108
CVE-2014-3488.....	109
CVE-2014-0114.....	110
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.....	120
CVE-2010-2197.....	121
CVE-2010-2059.....	123
CVE-2009-3014.....	124
CVE-2009-3010.....	125
CVE-2009-1251.....	126
CVE-2008-6161.....	128
CVE-2008-2503.....	129
CVE-2008-2298.....	130
CVE-2008-0501.....	131
CVE-2007-6640.....	132
CVE-2007-4039.....	133
CVE-2007-1794.....	135
CVE-2007-1466.....	136
CVE-2007-1157.....	137

CVE-2007-1137.....	138
CVE-2006-6498.....	139
CVE-2006-5562.....	141
CVE-2006-1547.....	142
CVE-2006-0496.....	143
CVE-2005-4889.....	144
CVE-2005-4837.....	146
CVE-2005-4685.....	147
CVE-2005-3896.....	148
CVE-2005-2270.....	149
CVE-2005-2269.....	150
CVE-2005-2268.....	152
CVE-2005-2266.....	153
CVE-2005-2265.....	154
CVE-2005-2263.....	155
CVE-2005-2261.....	156
CVE-2005-2260.....	157
CVE-2005-1937.....	159
CVE-2005-1532.....	160
CVE-2005-1531.....	161
CVE-2005-1160.....	162
CVE-2005-1159.....	163
CVE-2005-1157.....	164
CVE-2005-1156.....	166
CVE-2005-1155.....	167
CVE-2005-1154.....	168
CVE-2005-1153.....	169
CVE-2005-0593.....	170
CVE-2005-0592.....	171
CVE-2005-0590.....	172
CVE-2005-0588.....	174
CVE-2005-0586.....	175
CVE-2005-0585.....	176
CVE-2005-0584.....	177
CVE-2005-0578.....	178
CVE-2005-0401.....	179
CVE-2005-0399.....	180
CVE-2005-0149.....	182
CVE-2005-0147.....	183
CVE-2005-0146.....	184
CVE-2005-0144.....	185
CVE-2005-0143.....	186
CVE-2005-0142.....	187
CVE-2005-0141.....	188
CVE-2004-1614.....	189
CVE-2004-1613.....	191
CVE-2004-1450.....	192
CVE-2004-1381.....	193
CVE-2004-1380.....	194
CVE-2004-1316.....	195
CVE-2004-1156.....	196
CVE-2004-0909.....	197
CVE-2004-0908.....	199
CVE-2004-0907.....	200
CVE-2004-0906.....	201
CVE-2004-0905.....	202
CVE-2004-0904.....	203
CVE-2004-0903.....	204
CVE-2004-0902.....	205

io.grpc:grpc-netty.....	243
Netty/Common.....	244
Netty/Transport/Native/Unix/Common.....	245
CDI APIs.....	245
JTidy.....	246
Lucene Common Analyzers.....	247
Lucene Memory.....	247
Lucene Core.....	248
Lucene Queries.....	248
Lucene QueryParsers.....	249
Lucene Sandbox.....	249
Doxia :: Core.....	249
Doxia Sitetools :: Decoration Model.....	250
Doxia Sitetools :: Integration Tools.....	250
Doxia :: Logging API.....	250
Doxia :: XHTML5 Module.....	251
Doxia :: XHTML Module.....	251
Doxia :: Sink API.....	252
Doxia Sitetools :: Site Renderer.....	252
Doxia Sitetools :: Skin Model.....	252
Maven Plugin Tools Java 5 Annotations.....	253
Maven Plugin Tool for Java with Annotations.....	253
Maven Plugin Tools Extractor API.....	253
Maven Plugin Tools Generators.....	254
Maven Plugin Tool for Java with Javadoc Tags.....	254
Maven Plugin Plugin.....	255
Apache Maven Reporting API.....	255
Apache Maven Reporting Implementation.....	255
Apache Maven Wagon :: API.....	256
Maven Aether Provider.....	256
Maven Artifact.....	256
Maven Compat.....	257
Maven Core.....	257
Maven Model Builder.....	258
Maven Model.....	258
Maven Plugin API.....	258
Maven Repository Metadata Model.....	259
Maven Settings Builder.....	259
Maven Settings.....	259
Apache Thrift.....	260
VelocityTools.....	261
\${project.groupId}:\${project.artifactId}.....	261
Plexus Common Utilities.....	262
Plexus Archiver Component.....	263
snappy.....	263
JDOM.....	264
Mozilla Rhino.....	264
XZ for Java.....	271
Xalan Java Serializer.....	271

5 ae-artifact-analysis Vulnerability Notice.....272

6 ae-artifact-analysis Vulnerability List.....272

Applicable.....	272
In Review.....	272
Not Applicable.....	281
Insignificant.....	281

Void.....290

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

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

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

In Review **Default** **High**

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

Criteria	Explanation
CVSS Overall	CVSS:4.0 <i>GitHub, Inc.</i> 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

Deserialization 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

In Review

Default

High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

References

Affected Components

Weakness

CWE-502

Initial Severity

Advisories

Alerts

Assessment

Summary

CVSS Vector Severity Charts

Rationale

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

Plexus 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

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

Assessment

Summary

Critical

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

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

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

Assessment

Summary

High

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-6mjg-h674-j845	netty-handler SniHandler 16MB allocation	2023-06-20	2023-06-20

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: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 variants 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...

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

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

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

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

In Review **Default** **High**

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 .

© `\documentcopyrightyear` `\organizationname`

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

Id	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

☐ Insignificant
 ☐ Default
 ☒ Medium

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 .

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.

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

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

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

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

☐ Insignificant
 ☐ Default
 ☒ Medium

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 .

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

Id	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

Score is below 7,0

No elevated priority.

CWE-681

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

Alerts

Id	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

Summary

In Review **Default** **High**

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

Description

Netty is an open-source, asynchronous event-driven network application framework. The package `io.netty:netty-codec-http` 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

Id	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

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 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

ID	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

High

CVSS Vector Severity Charts

CWE-341, CWE-330

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

Alerts

Id	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

Summary

Medium

Score is below 7,0

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: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

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

References

Affected Components

Weakness

Initial Severity

Advisories

Alerts

Assessment

Summary

High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

No elevated priority.

Doc. Version: \${document.version}

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

Id	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

High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Default

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 .

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

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

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

ID	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

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

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

ID	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

Insignificant
Default
Medium

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 .

CWE-611

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

Alerts

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

Summary

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: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-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

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

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

In Review **Default** **Critical**

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 .

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

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

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

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

Insignificant
Default
Medium

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 .

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

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

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

Insignificant **Default** **Medium**

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

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

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

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

☐ Insignificant
 ☐ Default
 ☒ Low

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 .

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

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

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

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

In Review **Default** **Critical**

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 .

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

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

☐ Insignificant
 ☐ Default
 ☒ Medium

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 .

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

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

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

Alerts

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

Summary

In Review **Default** **Critical**

Rationale

The vulnerability has automatically been marked as in review.

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 0.53 % 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 .

© \${document.copyright.year} \${organization.name}

Critical

No elevated priority.

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. 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.	2022-05-24	2022-05-24

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: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

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

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: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 .

Alerts

© \${document.copyright.year} \${organization.name}

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-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

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: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

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

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

ID	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

In Review **Default** **High**

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 .

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

In Review

Default

Critical

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

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

In Review **Default** **High**

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 .

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

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

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

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

In Review **Default** **High**

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 .

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

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

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: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

Component	Artifact Id	Version
	dom4j-1.6.1.jar	1.6.1

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

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

In Review **Default** **High**

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 .

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

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

Critical

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 .

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

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

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

Id	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

In Review **Default** **Critical**

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

Id	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

In Review

Default

High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

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

Alerts

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

CWE-476

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

Alerts

Id	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

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: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

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.

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

Component	Artifact Id	Version
	tools-1.8.0.jar	1.8.0

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

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

Insignificant
Default
Medium

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.

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

Id	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

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

ID	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

CWE-189

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

Alerts

ID	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

Summary

In Review **Default** **Critical**

CVSS Vector Severity Charts

The vulnerability has automatically been marked as in review.

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

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

Id	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 .

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

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

Assessment

Summary

Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

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

Id	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

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: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

Alerts

ID	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

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

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

Alerts

ID	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

Summary

Insignificant
Default
Medium

CVSS Vector Severity Charts

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 .

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

Id	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

Alerts

ID	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

Summary

Default

High

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

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

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

ID	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 ;~ (semicolon tilde) sequence in a Name tag.	2022-05-17	2022-05-17

☐ Insignificant
 ☐ Default
 ☒ Medium

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: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

Id	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

In Review

Default

High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default

No elevated priority.

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

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

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

ID	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

In Review **Default** **Critical**

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.

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	<div>Medium</div>

Advisories

Alerts

Id	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

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 42.07 % 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

ID	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

Critical

CVSS Vector Severity Charts

CWE-264

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

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

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 0.46 % 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

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 0.09 % 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

In Review **Default** **Critical**

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 1.60 % 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

Alerts

Id	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

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

Id	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

☐ Insignificant
 ☐ Default
 ☒ Medium

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 .

© \${document.copyright.year} \${organization.name}

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

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

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

ID	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

Insignificant Due Medium

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 .

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-7qvv-cwgj-c8rj	Improper Input Validation in Apache Struts	2022-05-01	2022-05-01

Assessment

Summary

High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

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

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

ID	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

In Review **Default** **High**

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 .

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 .

CVE-2005-4685

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

Alerts

Id	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

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

ID	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

In Review **Default** **High**

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 .

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

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

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

ID	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

In Review **Default** **High**

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 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 .

CVE-2005-2268

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
---------------	---------	-----

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 .

CVE-2005-2266

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

Medium

CVSS Vector Severity Charts

Score is below 7,0

No elevated priority.

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

Id	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

In Review **Default** **High**

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 .

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

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

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

ID	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 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.	2022-05-01	2022-05-01

In Review **Default** **High**

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 2.31 % 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 .

CVE-2005-1937

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

Id	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 re-introduction 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.

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 .

CVE-2005-1532

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

High

CVSS Vector Severity Charts

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

Id	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

In Review **Default** **High**

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 .

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

Id	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

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 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 .

CVE-2005-1156

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

Id	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

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 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 .

CVE-2005-1155

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

Id	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

High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Escalate (9.2 from base score 7.5)

© \${document.copyright.year} \${organization.name}

Advisories

Alerts

Id	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

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

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

Id	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

In Review **Default** **High**

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 .

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.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0590

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

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

ID	Summary	Create Date	Update Date
GHSA-mq4v-fvj7-qhmq	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

☐ Insignificant
 ☐ Default
 ☒ Medium

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 .

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 0.09 % 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

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

Id	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

☐ Insignificant
 ☐ Default
 ☒ Medium

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 .

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

Id	Summary	Create Date	Update Date
GHSA-x75c-2774-mpv3	Heap-based buffer overflow in GIF2.cpp in Firefox before 1.0.2, Mozilla before 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

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 .

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

ID	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

☐ Insignificant
 ☐ Default
 ☒ Low

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 .

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2005-0141

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-1614

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

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

Id	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

☐ Insignificant
 ☐ Default
 ☒ Medium

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 .

CVE-2004-1613

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

Id	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.

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 .

CVE-2004-1450

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

ID	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

☐ Insignificant
 ☐ Default
 ☒ Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

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

Score is below 7,0

No elevated priority.

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

Summary

Medium

Score is below 7,0

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 .

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

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-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.

CVE-2004-0908

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

Id	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

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.

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 .

CVE-2004-0907

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	<div>Medium</div>

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

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

ID	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

Medium

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-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

In Review

Default

Critical

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

Id	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

In Review

Escalate

Critical

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 .

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 .

CVE-2004-0764

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

Id	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

In Review

Default

Critical

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

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

ID	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

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

ID	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

☐ Insignificant
 ☐ Default
 ☒ Medium

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 .

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0758

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

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

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

Insignificant **Default** **Medium**

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 .

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.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2004-0757

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

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

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

In Review **Default** **Critical**

The vulnerability has automatically been marked as in review.

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 .

Component	Artifact Id	Version
JTidy	jtidy-r938.jar	r938

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

Id	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

In Review **Default** **High**

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 .

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.

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2000-0655

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

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

Id	Summary	Create Date	Update Date
GHSA-5cwq-wmjk-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

Insignificant
Default
Medium

Score is below 7.0

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 .

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-rcqp					
	cpe:/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-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 6: json-schema-core Vulnerabilities

btfl

Artifacts

Component	Artifact Id	Version
btfl	btfl-1.3.jar	1.3

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-10519	8.8		<div>High</div>		<div>Default</div>	<div>In Review</div>

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-10518	8.8		High		Default	In Review
CVE-2020-10517	4.3		Medium		Default	Insignificant

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
CVE-2020-10518	8.8		High		Default	In Review
CVE-2020-10517	4.3		Medium		Default	Insignificant
CVE-2012-2055	7.5		High		Default	In Review

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-rcqp						
cpe:/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-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 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

Vulnerabilities

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						

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-25738	6.7		Medium		Default	Insignificant
GHSA-m8wh-mqgf-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

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2020-8554	5.0		Medium		Default	Insignificant

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Metrics	kubernetes-model-metrics-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 34: Fabric8 :: Kubernetes Model :: Metrics Vulnerabilities

Artifacts

Component	Artifact Id	Version
Fabric8 :: Kubernetes Model :: Networking	kubernetes-model-networking-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 35: Fabric8 :: Kubernetes Model :: Networking Vulnerabilities

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						

Artifacts

Vulnerabilities

© `\documentcopyrightyear` `\organizationname`

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.jar	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

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2005-4837	GHSA-wxm5-2gcr-wvxp					
	cpe:/a:open_source_technology_group:sourceforge:1.0.4 1.0.4 (*)					
	10.0		Critical		Default	In Review
CVE-2002-2364	GHSA-m3xm-f262-69qm					
	cpe:/a:sourceforge:net-snmp [, 5.0.9]					
	4.3		Medium		Default	Insignificant
CVE-2002-2362	GHSA-cxx3-573v-vcgm					
	cpe:/a:sourceforge:php_ticket [, 0.5]					
	4.3		Medium		Default	Insignificant
CVE-2001-0234	GHSA-rhp6-27r4-xwgx					
	cpe:/a:sourceforge:mymarket:1.71 1.71 (*)					
	7.5		High		Default	In Review
	GHSA-9xw2-c3qj-x8m5					
	cpe:/a:sourceforge:newsdaemon:0.21b 0.21b (*)					

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:lucene [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

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

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 66: Maven Plugin Tool for Java with Javadoc Tags Vulnerabilities

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 org.apache.maven:maven-core (Maven) [0, 3.8.1)						

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 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:thrift [, 2021.02.22.00)						
CVE-2019-3565	7.5		High		Default	In Review
GHSA-j98f-h9mx-xrxq						
cpe:/a:facebook:thrift [, 2019.05.06.00)						
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:thrift [, 2019.02.18.00)						
CVE-2019-3558	7.5		High		Default	In Review
GHSA-7vv7-v9gp-whmr						
cpe:/a:facebook:thrift [, 2019.02.18.00)						
CVE-2019-3553	7.5		High		Default	In Review
GHSA-859v-9mcv-7rw3						
cpe:/a:facebook:thrift [, 2020.02.03.00)						
CVE-2019-3552	7.5		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-h27g-g76x-xqpw					
	cpe:/a:facebook:thrift [, 2019.02.18.00)					
CVE-2019-11939	7.5		High		Default	In Review
	GHSA-w3r9-r9w7-8h48					
	cpe:/a:facebook:thrift [, 2020.03.16.00)					
CVE-2019-11938	7.5		High		Default	In Review
	GHSA-hr4p-8hm2-w85x					
	cpe:/a:facebook:thrift [, 2019.12.09.00)					

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

Artifacts

Component	Artifact Id	Version
<div></div> <div></div> <div></div>	batik-anim-1.14.jar	1.14
<div></div> <div></div> <div></div>	batik-awt-util-1.14.jar	1.14
<div></div> <div></div> <div></div>	batik-bridge-1.14.jar	1.14
<div></div> <div></div> <div></div>	batik-codec-1.14.jar	1.14
<div></div> <div></div> <div></div>	batik-constants-1.14.jar	1.14
<div></div> <div></div> <div></div>	batik-css-1.14.jar	1.14
<div></div> <div></div> <div></div>	batik-dom-1.14.jar	1.14
<div></div> <div></div> <div></div>	batik-ext-1.14.jar	1.14
<div></div> <div></div> <div></div>	batik-gvt-1.14.jar	1.14

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2005-2260	7.5		High		Default	In Review
	GHSA-wm6x-mrp3-f56m					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1937	2.6		Low		Default	Insignificant
	GHSA-ffxc-32xj-v3rp					
	cpe:/a:mozilla:mozilla:1.7.7 1.7.7 (*)					
CVE-2005-1532	7.5		High		Due	In Review
	GHSA-ffv2-fj33-mvch					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1531	7.5		High		Default	In Review
	GHSA-q7v5-vf67-fpfr					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1160	5.1		Medium		Default	Insignificant
	GHSA-r5gq-7c27-jhm8					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1159	7.5		High		Default	In Review
	GHSA-65q8-rprw-c44f					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1157	7.5		High		Default	In Review
	GHSA-8hfq-wv6x-73v6					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1156	7.5		High		Default	In Review
	GHSA-p7cq-vpx5-5pp5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1155	7.5		High		Escalate	In Review
	GHSA-5f3p-wqh5-33m5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1154	7.5		High		Default	In Review
	GHSA-xrcj-fc8v-w45w					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-1153	7.5		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2005-0593	GHSA-9j3v-w638-mx3p					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0592	2.6		Low		Default	Insignificant
	GHSA-74mv-jc74-mg2v					
CVE-2005-0590	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
CVE-2005-0588	GHSA-3fwv-8g5j-79jx					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0586	5.0		Medium		Default	Insignificant
	GHSA-mq4v-fvj7-qhmj					
CVE-2005-0585	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	5.0		Medium		Default	Insignificant
CVE-2005-0584	GHSA-g63h-wr5c-mmgm					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0578	2.6		Low		Default	Insignificant
	GHSA-wrw4-477q-3qjh					
CVE-2005-0584	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	2.6		Low		Default	Insignificant
CVE-2005-0584	GHSA-cxhx-r8q3-rf4p					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0584	2.6		Low		Default	Insignificant
	GHSA-v9x2-68hw-cwxx					
CVE-2005-0584	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	2.1		Low		Default	Insignificant
CVE-2005-0584	GHSA-7352-x97x-grpg					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0401	5.1		Medium		Default	Insignificant
	GHSA-p4xc-fq3x-cx45					
CVE-2005-0399	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	5.1		Medium		Elevated	Insignificant
CVE-2005-0399	GHSA-x75c-2774-mpv3					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2004-1381	5.0		Medium		Default	Insignificant
	GHSA-hhqx-qfww-wwhc					
	cpe:/a:mozilla:mozilla					
CVE-2004-1380	5.0		Medium		Default	Insignificant
	GHSA-vv9m-2w98-m7rf					
	cpe:/a:mozilla:mozilla					
CVE-2004-1316	5.0		Medium		Default	Insignificant
	GHSA-9c99-v6fv-f744					
	cpe:/a:mozilla:mozilla					
CVE-2004-1156	4.3		Medium		Default	Insignificant
	GHSA-g6f4-4jhr-qjg5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0909	5.1		Medium		Default	Insignificant
	GHSA-fmr4-hv22-46fr					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0908	4.0		Medium		Default	Insignificant
	GHSA-8c73-9gh8-7c8v					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0907	4.6		Medium		Default	Insignificant
	GHSA-jgmj-mpcg-qp5x					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0906	4.6		Medium		Default	Insignificant
	GHSA-2vph-3h86-9f5r					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0905	4.6		Medium		Default	Insignificant
	GHSA-fqjg-fc86-m5cr					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0904	10.0		Critical		Default	In Review
	GHSA-238r-rqpq-9cqf					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0903	10.0		Critical		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2004-0902	GHSA-q3j6-xfjj-26q5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0765	10.0		Critical		Escalate	In Review
	GHSA-53rc-xfx7-6qmc					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0764	7.5		High		Default	In Review
	GHSA-h29q-7v28-gprh					
	cpe:/a:mozilla:mozilla [, 1.7]					
CVE-2004-0762	10.0		Critical		Default	In Review
	GHSA-pw9h-wwm9-4h36					
	cpe:/a:mozilla:mozilla [, 1.7]					
CVE-2004-0761	5.0		Medium		Default	Insignificant
	GHSA-254j-3m2w-23xr					
	cpe:/a:mozilla:mozilla [, 1.7]					
CVE-2004-0760	5.0		Medium		Default	Insignificant
	GHSA-v4fj-43xc-9937					
	cpe:/a:mozilla:mozilla [, 1.7]					
CVE-2004-0759	6.4		Medium		Default	Insignificant
	GHSA-75wj-j7cg-5q44					
	cpe:/a:mozilla:mozilla					
CVE-2004-0758	6.4		Medium		Default	Insignificant
	GHSA-q2hq-vr9g-6x97					
	cpe:/a:mozilla:mozilla					
CVE-2004-0757	5.0		Medium		Default	Insignificant
	GHSA-6ccr-h2cv-pc67					
	cpe:/a:mozilla:mozilla					
CVE-2004-0478	10.0		Critical		Default	In Review
	GHSA-ffvj-mxf9-q65v					
	cpe:/a:mozilla:mozilla [, 1.7]					
CVE-2004-0478	2.6		Low		Default	Insignificant
	GHSA-5435-hp8c-m4q9					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2004-0902	GHSA-q3j6-xfjj-26q5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	10.0		Critical		Escalate	In Review
CVE-2004-0764	GHSA-53rc-xfx7-6qmc					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	10.0		Critical		Default	In Review
CVE-2004-0757	GHSA-pw9h-wwm9-4h36					
	cpe:/a:mozilla:mozilla [, 1.7]					
	10.0		Critical		Default	In Review
CVE-2023-41330	GHSA-ffvj-mxf9-q65v					
	cpe:/a:mozilla:mozilla [, 1.7]					
	9.8		Critical		Default	In Review
CVE-2023-37460	GHSA-92rv-4j2h-8mjj					
	cpe:/a:knplabs:snappy [, 1.4.3)					
	9.8		Critical		Default	In Review
CVE-2023-28115	GHSA-wh3p-fphp-9h2m					
	cpe:/a:codehaus-plexus:plexus-archiver [, 4.8.0), GHSA org.codehaus.plexus:plexus-archiver (Maven) [0, 4.8.0)					
	9.8		Critical		Default	In Review
CVE-2021-24028	GHSA-gq6w-q6wh-jggc					
	cpe:/a:knplabs:snappy [, 1.4.2)					
	9.8		Critical		Default	In Review
CVE-2020-7768	GHSA-qrr3-c36x-2pcc					
	cpe:/a:facebook:thrift [, 2021.02.22.00)					
	9.8		Critical		Default	In Review
CVE-2020-10683	GHSA-pp75-xfpw-37g9					
	cpe:/a:grpc:grpc:::~~~node.js~~ [, 1.1.8)					
	9.8		Critical		Default	In Review
CVE-2017-9431	GHSA-hwj3-m3p6-hj38					
	cpe:/a:dom4j_project:dom4j [, 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3)					
	9.8		Critical		Default	In Review
	GHSA-6q3h-fg8c-jqrj					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2017-8359	cpe:/a:grpc:grpc [1.2.2]					
	9.8		Critical		Default	In Review
	GHSA-j2fw-rfr9-pfrh					
CVE-2017-7861	cpe:/a:grpc:grpc [1.2.1]					
	9.8		Critical		Default	In Review
	GHSA-wgxc-2fq5-r7v3					
CVE-2017-7860	cpe:/a:grpc:grpc [1.1.2]					
	9.8		Critical		Default	In Review
	GHSA-j8v6-6xq3-6m4f					
CVE-2017-1000487	cpe:/a:grpc:grpc [1.1.2]					
	9.8		Critical		Default	In Review
	GHSA-8vhq-qq4p-grq3					
CVE-2011-3378	cpe:/a:codehaus-plexus:plexus-utils [3.0.16), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.16)					
	9.3		Critical		Default	In Review
	GHSA-34ff-v8wx-w9f5					
CVE-2008-2503	cpe:/a:rpm:rpm [4.9.1.1]					
	9.3		Critical		Default	In Review
	GHSA-jxq6-p7m9-896m					
CVE-2021-26291	cpe:/a:sourceforge:emule_x-ray:1.2 1.2 (*)					
	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
CVE-2020-8570	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)					
	9.1		Critical		Default	In Review
	GHSA-cghx-9gcr-r42x					
CVE-2019-20445	cpe:/a:kubernetes:java [9.0.2)					
	9.1		Critical		Default	In Review
	GHSA-p2v9-g2qv-p635					
CVE-2019-20444	cpe:/a:netty:netty [4.1.44)					
	9.1		Critical		Default	In Review
	GHSA-cqqj-4p63-rrmm					
	cpe:/a:netty:netty [4.1.44)					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2022-1271	8.8		High		Default	In Review
	GHSA-jrpw-543v-8r62					
	cpe:/a:tukaani:xz [, 5.2.5)					
CVE-2020-13936	8.8		High		Default	In Review
	GHSA-59j4-wjwp-mw9m					
	GHSA org.apache.velocity:velocity (Maven) [0, 1.7]					
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					
	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-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]					
CVE-2005-3896	7.8		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2013-6435	GHSA-f389-88pf-8hp7					
	cpe:/a:mozilla:mozilla					
	7.6		High		Default	In Review
CVE-2007-1157	GHSA-qww5-w98g-66q7					
	cpe:/a:rpm:rpm [, 4.11.1]					
	7.6		High		Default	In Review
CVE-2023-3635	GHSA-r86m-hxp8-3mvw					
	cpe:/a:jboss:jboss					
	7.5		High		Default	In Review
CVE-2023-34623	GHSA-w33c-445m-f8w7					
	cpe:/a:squareup:okio [0.5.0, 1.17.6), GHSA com.squareup.okio:okio (Maven) [0, 1.17.6)					
	7.5		High		Default	In Review
CVE-2023-33953	GHSA-fv2r-hw24-8rxj					
	cpe:/a:jtidy_project:jtidy [, r938]					
	7.5		High		Default	In Review
CVE-2022-4244	GHSA-496j-2rq6-j6cc					
	cpe:/a:grpc:grpc::~~~~~ [, 1.53.2)					
	7.5		High		Default	In Review
CVE-2022-41881	GHSA-g6ph-x5wf-g337					
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.24), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.24)					
	7.5		High		Default	In Review
CVE-2022-34169	GHSA-fx2c-96vj-985v					
	cpe:/a:netty:netty [, 4.1.86)					
	7.5		High		Default	In Review
CVE-2021-37137	GHSA-9339-86wc-4qgf					
	cpe:/a:apache:xalan-java [, 2.7.2], GHSA xalan:xalan (Maven) [0, 2.7.3)					
	7.5		High		Default	In Review
CVE-2021-37136	GHSA-9vjp-v76f-g363					
	cpe:/a:netty:netty [, 4.1.68)					
	7.5		High		Default	In Review
GHSA-grg4-wf29-r9vv						

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-33813	cpe:/a:netty:netty [, 4.1.68)					
	7.5		High		Default	In Review
	GHSA-2363-cqg2-863c					
CVE-2019-3565	cpe:/a:jdom:jdom [, 2.0.6]					
	7.5		High		Default	In Review
	GHSA-j98f-h9mx-xrxq					
CVE-2019-3564	cpe:/a:facebook:thrift [, 2019.05.06.00)					
	7.5		High		Default	In Review
	GHSA-x4rg-4545-4w7w					
CVE-2019-3559	cpe:/a:facebook:thrift [, 2019.03.04.00)					
	7.5		High		Default	In Review
	GHSA-6627-jcx5-j2g8					
CVE-2019-3558	cpe:/a:facebook:thrift [, 2019.02.18.00)					
	7.5		High		Default	In Review
	GHSA-7vv7-v9gp-whmr					
CVE-2019-3553	cpe:/a:facebook:thrift [, 2019.02.18.00)					
	7.5		High		Default	In Review
	GHSA-859v-9mcv-7rw3					
CVE-2019-3552	cpe:/a:facebook:thrift [, 2020.02.03.00)					
	7.5		High		Default	In Review
	GHSA-h27g-g76x-xqpw					
CVE-2019-16869	cpe:/a:facebook:thrift [, 2019.02.18.00)					
	7.5		High		Default	In Review
	GHSA-p979-4mfw-53vg					
CVE-2019-11939	cpe:/a:netty:netty [, 4.1.42)					
	7.5		High		Default	In Review
	GHSA-w3r9-r9w7-8h48					
CVE-2019-11938	cpe:/a:facebook:thrift [, 2020.03.16.00)					
	7.5		High		Default	In Review
	GHSA-hr4p-8hm2-w85x					
	cpe:/a:facebook:thrift [, 2019.12.09.00)					

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-f2rv					
	cpe:/a:netty:netty [, 3.9.7]					
CVE-2014-0114	7.5		High		Escalate	In Review
	GHSA-p66x-2cv9-qq3v					
	cpe:/a:apache:commons_beanutils [, 1.9.1]					
CVE-2012-2055	7.5		High		Default	In Review
	GHSA-8qp2-79w8-8586					
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)					
CVE-2008-2298	7.5		High		Default	In Review
	GHSA-39wm-cmp6-6mjc					
	cpe:/a:sourceforge:web_slider:0.6 0.6 (*)					
CVE-2006-5562	7.5		High		Default	In Review
	GHSA-wxm5-2gcr-wvxp					
	cpe:/a:open_source_technology_group:sourceforge:1.0.4 1.0.4 (*)					
CVE-2006-1547	7.5		High		Escalate	In Review
	GHSA-7qvv-cwgj-c8rj					
	cpe:/a:apache:commons_beanutils:1.7.0 1.7.0 (*)					
CVE-2005-2270	7.5		High		Default	In Review
	GHSA-jgwp-9p3p-4h7j					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-2269	7.5		High		Default	In Review
	GHSA-cxw5-72vp-8h54					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-2261	7.5		High		Default	In Review
	GHSA-j45r-pcwj-8g72					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-2260	7.5		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2005-1532	GHSA-wm6x-mrp3-f56m					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Due	In Review
CVE-2005-1531	GHSA-ffv2-fj33-mvch					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
CVE-2005-1159	GHSA-q7v5-vf67-fpfr					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
CVE-2005-1157	GHSA-65q8-rprw-c44f					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
CVE-2005-1156	GHSA-8hfq-wv6x-73v6					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
CVE-2005-1155	GHSA-p7cq-vpx5-5pp5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Escalate	In Review
CVE-2005-1154	GHSA-5f3p-wqh5-33m5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
CVE-2005-1153	GHSA-xrcj-fc8v-w45w					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
CVE-2005-0592	GHSA-9j3v-w638-mx3p					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
CVE-2005-0147	GHSA-3fwv-8g5j-79jx					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	7.5		High		Default	In Review
	GHSA-25p3-2r5q-956q					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0765	7.5		High		Default	In Review
	GHSA-h29q-7v28-gprh					
	cpe:/a:mozilla:mozilla [, 1.7]					
CVE-2002-0815	7.5		High		Default	In Review
	GHSA-6p7q-r2p3-gx4g					
	cpe:/a:mozilla:mozilla					
CVE-2001-0234	7.5		High		Default	In Review
	GHSA-9xw2-c3qj-x8m5					
	cpe:/a:sourceforge:newsdaemon:0.21b 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-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-pmxj					
	cpe:/a:rpm:rpm [, 4.4.2.3]					
CVE-2023-2976	7.1		High		Default	In Review
	GHSA-7g45-4rm6-3mm3					
	cpe:/a:google:guava [, 32.0.0)					
CVE-2022-44729	7.1		High		Default	In Review
	GHSA-gq5f-xv48-2365					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-47535	GHSA org.apache.xmlgraphics:batik-bridge (Maven) [1.0, 1.17), GHSA org.apache.xmlgraphics:batik-transcoder (Maven) [1.0, 1.17)					
	7.0		High		Default	In Review
	GHSA-xq3w-v528-46rv					
CVE-2018-6969	GHSA io.netty:netty-common (Maven) [0, 4.1.115)					
	7.0		High		Default	In Review
	GHSA-qc3q-9h28-r994					
CVE-2023-45960	cpe:/a:vmware:tools [, 10.3.0)					
					Default	In Review
	GHSA-fgq9-fc3q-vqmw					
	GHSA org.dom4j:dom4j (Maven) [0, 2.1.4]					

Table 91: In Review Category (ae-artifact-analysis)

Not Applicable

No vulnerabilities are considered Not Applicable within the given configuration.

Insignificant

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-2023-074					
	GHSA-qppj-fm5r-hxr3					
CVE-2012-0815	cpe:/a:grpc:grpc::~~go~~ [, 1.56.3), cpe:/a:netty:netty [, 4.1.100)					
	6.8		Medium		Default	Insignificant
	CERT-EU-2012-0126					
CVE-2012-0061	GHSA-6grx-55mc-2wmq					
	cpe:/a:rpm:rpm [, 4.9.1.2]					
	6.8		Medium		Default	Insignificant
CVE-2012-0060	CERT-EU-2012-0126					
	GHSA-v3v4-hffr-vr89					
	cpe:/a:rpm:rpm [, 4.9.1.2]					
	6.8		Medium		Default	Insignificant

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	CERT-EU-2012-0126					
	GHSA-j6wj-cqmg-hvcm					
	cpe:/a:rpm:rpm [, 4.9.1.2]					
CVE-2007-1466	6.8		Medium		Default	Insignificant
	GHSA-mc39-g53r-8cq4					
	cpe:/a:sourceforge:wordperfect_document_importer-exporter [, 0.8.8]					
CVE-2006-6498	6.8		Medium		Due	Insignificant
	GHSA-jmfp-6hwg-w7qf					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2021-35939	6.7		Medium		Default	Insignificant
	GHSA-prgv-w33h-5m73					
	cpe:/a:rpm:rpm [, 4.18)					
CVE-2021-35938	6.7		Medium		Default	Insignificant
	GHSA-83gm-5269-qr3v					
	cpe:/a:rpm:rpm [, 4.18.0)					
CVE-2021-25738	6.7		Medium		Default	Insignificant
	GHSA-m8wh-mqgf-rr8g					
	cpe:/a:kubernetes:java [, 9.0.2]					
CVE-2015-5191	6.7		Medium		Default	Insignificant
	GHSA-4vr2-36wr-v82r					
	cpe:/a:vmware:tools [, 10.0.8]					
CVE-2023-34462	6.5		Medium		Default	Insignificant
	GHSA-6mj-q-h674-j845					
	cpe:/a:netty:netty [, 4.1.94)					
CVE-2021-43797	6.5		Medium		Default	Insignificant
	GHSA-wx5j-54mm-rqqq					
	cpe:/a:netty:netty [, 4.1.71)					
CVE-2021-35937	6.4		Medium		Default	Insignificant
	GHSA-63x9-9q4w-j636					
	cpe:/a:rpm:rpm [, 4.18.0)					
CVE-2007-6640	6.4		Medium		Default	Insignificant

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-jmrg-23pg-v7hm					
	cpe:/a:sourceforge:creammonkey:0.9 0.9 (*), cpe:/a:sourceforge:greasekit:1.2 1.2 (*)					
CVE-2005-4685	6.4		Medium		Default	Insignificant
	GHSA-qx3r-96cr-cwr5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-0760	6.4		Medium		Default	Insignificant
	GHSA-75wj-j7cg-5q44					
	cpe:/a:mozilla:mozilla					
CVE-2004-0759	6.4		Medium		Default	Insignificant
	GHSA-q2hq-vr9g-6x97					
	cpe:/a:mozilla:mozilla					
CVE-2014-4199	6.3		Medium		Default	Insignificant
	GHSA-v55p-68fc-xxcv					
	cpe:/a:vmware:tools					
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]					
CVE-2021-21409	5.9		Medium		Default	Insignificant
	GHSA-f256-j965-7f32					
	cpe:/a:netty:netty [, 4.1.61)					
CVE-2021-21295	5.9		Medium		Default	Insignificant
	GHSA-wm47-8v5p-wjpj					
	cpe:/a:netty:netty [, 4.1.60)					
CVE-2010-2197	5.8		Medium		Default	Insignificant
	GHSA-6gj2-w23f-chf3					
	cpe:/a:rpm:rpm [, 4.8.0]					
CVE-2008-0501	5.8		Medium		Default	Insignificant
	GHSA-q7mg-4q42-3h7f					
	cpe:/a:sourceforge:phpmyclub:0.0.1 0.0.1 (*)					
CVE-2023-0833	5.5		Medium		Default	Insignificant
	GHSA-8fhc-q55v-jvx2					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:squareup:okhttp [, 4.9.2)					
CVE-2022-24823	5.5		Medium		Default	Insignificant
	GHSA-269q-hmxg-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:tools [, 10.0.8]					
CVE-2024-36124	5.3		Medium		Default	Insignificant
	GHSA-8wh2-6qhj-h7j9					
	GHSA org.iq80.snappy:snappy (Maven) [0, 0.5)					
CVE-2023-32732	5.3		Medium		Default	Insignificant
	GHSA-9hxf-ppjv-w6rq					
	cpe:/a:grpc:grpc [, 1.53.0)					
CVE-2021-4277	5.3		Medium		Default	Insignificant
	GHSA-3cqm-26w8-85g8					
	cpe:/a:utils_project:utils [, 2021-05-14)					
CVE-2005-1160	5.1		Medium		Default	Insignificant
	GHSA-r5gq-7c27-jhm8					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0401	5.1		Medium		Default	Insignificant
	GHSA-p4xc-fq3x-cx45					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0399	5.1		Medium		Elevated	Insignificant
	GHSA-x75c-2774-mpv3					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2004-0909	5.1		Medium		Default	Insignificant
	GHSA-fmr4-hv22-46fr					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2020-8554	5.0		Medium		Default	Insignificant
	GHSA-j9wf-vvm6-4r9w					
	cpe:/a:kubernetes:kubernetes					
CVE-2014-3488	5.0		Medium		Default	Insignificant
	GHSA-9959-6p3m-wxpc					
	cpe:/a:netty:netty [, 3.9.1.1]					
CVE-2007-1137	5.0		Medium		Default	Insignificant
	GHSA-x927-rp8j-62cg					
	cpe:/a:sourceforge:putmail:.8 .8 (*)					
CVE-2005-2266	5.0		Medium		Default	Insignificant
	GHSA-gp89-32gv-6hww					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-2265	5.0		Medium		Elevated	Insignificant
	GHSA-5pgg-4c5c-9j5p					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-2263	5.0		Medium		Default	Insignificant
	GHSA-5v66-4mqr-49xj					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0590	5.0		Medium		Default	Insignificant
	GHSA-mq4v-fvj7-qhmj					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0588	5.0		Medium		Default	Insignificant
	GHSA-g63h-wr5c-mmgm					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0149	5.0		Medium		Default	Insignificant
	GHSA-2x58-77jw-wgpw					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0146	5.0		Medium		Default	Insignificant

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2004-1614	GHSA-pfw3-m738-qjww					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	5.0		Medium		Default	Insignificant
CVE-2004-1613	GHSA-cfrm-mc6g-2q3f					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	5.0		Medium		Default	Insignificant
CVE-2004-1450	GHSA-pqwg-424h-mwmq					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	5.0		Medium		Default	Insignificant
CVE-2004-1381	GHSA-9hj8-rmm5-7rx3					
	cpe:/a:mozilla:mozilla:1.7:beta 1.7 (beta)					
	5.0		Medium		Default	Insignificant
CVE-2004-1380	GHSA-hhqx-qfww-wwhc					
	cpe:/a:mozilla:mozilla					
	5.0		Medium		Default	Insignificant
CVE-2004-1316	GHSA-vv9m-2w98-m7rf					
	cpe:/a:mozilla:mozilla					
	5.0		Medium		Default	Insignificant
CVE-2004-0762	GHSA-9c99-v6fv-f744					
	cpe:/a:mozilla:mozilla					
	5.0		Medium		Default	Insignificant
CVE-2004-0761	GHSA-254j-3m2w-23xr					
	cpe:/a:mozilla:mozilla [, 1.7]					
	5.0		Medium		Default	Insignificant
CVE-2004-0758	GHSA-v4fj-43xc-9937					
	cpe:/a:mozilla:mozilla [, 1.7]					
	5.0		Medium		Default	Insignificant
CVE-2000-0655	GHSA-6ccr-h2cv-pc67					
	cpe:/a:mozilla:mozilla					
	5.0		Medium		Default	Insignificant
	GHSA-5cwq-wmjx-47pq					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2009-3014	4.3		Medium		Default	Insignificant
	GHSA-xw9p-2mr3-g9mx					
	cpe:/a:mozilla:mozilla [, 1.7]					
CVE-2009-3010	4.3		Medium		Default	Insignificant
	GHSA-mv6q-6xwq-rrw9					
	cpe:/a:mozilla:mozilla [, 1.7.12]					
CVE-2008-6161	4.3		Medium		Default	Insignificant
	GHSA-682j-rhpc-phrj					
	cpe:/a:sourceforge:wow_raid_manager [, 3.5.0]					
CVE-2007-4039	4.3		Medium		Default	Insignificant
	GHSA-5qrv-2vjc-xwcq					
	cpe:/a:mozilla:mozilla					
CVE-2006-0496	4.3		Medium		Elevated	Insignificant
	GHSA-747m-cwr6-qmx3					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2004-1156	4.3		Medium		Default	Insignificant
	GHSA-g6f4-4jhr-qjg5					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2002-2364	4.3		Medium		Default	Insignificant
	GHSA-cxx3-573v-vcgm					
	cpe:/a:sourceforge:php_ticket [, 0.5]					
CVE-2002-2362	4.3		Medium		Default	Insignificant
	GHSA-rhp6-27r4-xwgx					
	cpe:/a:sourceforge:mymarket:1.71 1.71 (*)					
CVE-2004-0908	4.0		Medium		Default	Insignificant
	GHSA-8c73-9gh8-7c8v					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2020-8908	3.3		Low		Default	Insignificant
	GHSA-5mg8-w23w-74h3					
	cpe:/a:google:guava [, 32.0.0)					
CVE-2005-2268	2.6		Low		Default	Insignificant

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2005-1937	GHSA-3937-9m84-64gp					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0593	2.6		Low		Default	Insignificant
	GHSA-ffxc-32xj-v3rp					
CVE-2005-0586	cpe:/a:mozilla:mozilla:1.7.7 1.7.7 (*)					
	2.6		Low		Default	Insignificant
CVE-2005-0585	GHSA-74mv-jc74-mg2v					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0584	2.6		Low		Default	Insignificant
	GHSA-wrw4-477q-3qjh					
CVE-2005-0144	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	2.6		Low		Default	Insignificant
CVE-2005-0143	GHSA-cxhx-r8q3-rf4p					
	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
CVE-2005-0141	2.6		Low		Default	Insignificant
	GHSA-gj3c-pxvc-4hrq					
CVE-2004-0478	cpe:/a:mozilla:mozilla					
	2.6		Low		Default	Insignificant
CVE-2005-0578	GHSA-8f62-jh9f-ffg5					
	cpe:/a:mozilla:mozilla					
CVE-2005-0578	2.6		Low		Default	Insignificant
	GHSA-jj36-3392-jhm7					
CVE-2005-0578	cpe:/a:mozilla:mozilla:1.7 1.7 (*)					
	2.6		Low		Default	Insignificant
CVE-2005-0578	GHSA-5435-hp8c-m4q9					
	cpe:/a:mozilla:mozilla					
CVE-2005-0578	2.1		Low		Default	Insignificant
	GHSA-7352-x97x-grpg					

