Doc. Identifier: \${document.id}

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

\${document.name}

Doc. Identifier: \${document.id}

Doc. Version: \${document.version}

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

Contents

1	ae-dita	Security Advisories	4
_	4:4-	Affected Accets	4
2	ae-dita	a Affected Assets	4
3	ae-dita	a Vulnerability Details	4
	CVE-2024-	4-47554	4
		4-36124	
		4-25710	
		3-45960	
	CVE-2023-	3-41330	9
	CVE-2023-	3-37460	10
	CVE-2023-	3-28115	11
	CVE-2022-	2-1271	13
	CVE-2021-	1-36374	14
	CVE-2021-	1-36373	15
	CVE-2021-	1-36090	16
	CVE-2021-	1-35517	18
	CVE-2021-	1-35516	19
	CVE-2021-	1-35515	20
	CVE-2021-	1-34083	21
	CVE-2021-	1-29425	22
	CVE-2021-	1-26291	24
	CVE-2020-	0-8927	25
	CVE-2020-	0-1945	26
	CVE-2020-	0-13936	28
	CVE-2020-	0-10683	29
	CVE-2018-	8-15756	30
	CVE-2018-	8-1324	31
	CVE-2018-	8-1275	32
	CVE-2018-	8-1272	34
	CVE-2018-	8-1271	35
	CVE-2018-	8-1270	36
	CVE-2018-	8-1257	37
	CVE-2018-	8-1199	38
	CVE-2018-	8-11771	40
	CVE-2018-	8-11040	41
	CVE-2018-	8-1002200	42
	CVE-2018-	8-1000632	43
	CVE-2015-	5-7501	44
	CVE-2015-	5-6420	46
	CVE-2015-	5-4035	47
	CVE-2012-	2-5817	48
1	ap-dita	Affected Components	<i>1</i> 0
7			
		collections Library	
		s Collections	
		Commons IO	
		Ant Launcher	
	ADDUCTE ATT	\ LUVI	

Apache Commons Compress	52
Maven Plugin Tools Java 5 Annotations	
Apache Maven Wagon :: API	53
Maven Aether Provider	
Maven Artifact	54
Maven Compat	54
Maven Core	
Maven Model Builder	55
Maven Model	55
Maven Plugin API	56
Maven Repository Metadata Model	
Maven Settings Builder	56
Maven Settings	
Plexus Archiver Component	57
snappy	58
Spring Core	58
XZ for Java	59
	••
5 ae-dita Vulnerability Notice	60
O 194- W. Leevel 1994 - 1944	22
6 ae-dita Vulnerability List	
Applicable	
In Review	
Not Applicable	
Insignificant	
Void	64

1 ae-dita Security Advisories

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

New Security Advisories

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

Security Advisories in Review

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

Reviewed Security Advisories

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

Not relevant Security Advisories

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

Security Advisories Summary

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

2 ae-dita Affected Assets

No affected assets have been identified.

3 ae-dita Vulnerability Details

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

CVE-2024-47554

Description

Uncontrolled Resource Consumption vulnerability in Apache Commons IO. The org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input. This issue affects Apache Commons IO: from 2.0 before 2.14.0. Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2024-47554

Affected Components

Component	Artifact Id	Version
Apache Commons IO	commons-io-2.5.jar	2.5

Weakness

CWE-400

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:4.0	GitHub, Inc.	8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	High
CVSS:3.1	GitHub, Inc.	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	High

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-78wr-2p64-hpwj	Apache Commons IO: Possible denial of service attack on untrusted input to XmlStreamReader	2024-10-03	2024-10-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation	
CVSS Overall	CVSS:4.0 GitHub, Inc. provides the vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA: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 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-2024-36124

Description

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

References

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

Affected Components

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

Weakness

CWE-125

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant	Default	Medium
		1110 0110111

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2024-25710

Description

Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Apache Commons Compress. This issue affects Apache Commons Compress: from 1.3 through 1.25.0. Users are recommended to upgrade to version 1.26.0 which fixes the issue.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2024-25710

Affected Components

Component	Artifact Id	Version
Apache Commons Compress	commons-compress-1.11.jar	1.11

Weakness

CWE-835

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-4g9r-vxhx-9pgx	Apache Commons Compress: Denial of service caused by an infinite loop for a corrupted DUMP file	2024-02-19	2024-02-19

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

Doc. Identifier: \${document.id}

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

Criteria	Explanation
EPSS	This vulnerability has a 0.06 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 72.64 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2023-45960

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	dom4j-1.6.1.jar	1.6.1

Initial Severity

The vulnerability does not provide any CVSS severity information.

Advisories

Alerts

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

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	No CVSS vector available.

Doc. Identifier: \${document.id} \${document.name} Doc. Version: \${document.versions between the companies of the companies of

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

CVE-2023-41330

Description

knplabs/knp-snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. ## Issue On March 17th the vulnerability CVE-2023-28115 was disclosed, allowing an attacker to gain remote code execution through PHAR deserialization. Version 1.4.2 added a check `if (\strpos(\\$filename, 'phar://') === 0)` in the `prepareOutput` function to resolve this CVE, however if the user is able to control the second parameter of the `generateFromHtml()` function of Snappy, it will then be passed as the `\\$filename` parameter in the `prepareOutput()` function. In the original vulnerability, a file name with a `phar:// wrapper could be sent to the `fileExists()` function, equivalent to the `file_exists()` PHP function. This allowed users to trigger a deserialization on arbitrary PHAR files. To fix this issue, the string is now passed to the `strpos()` function and if it starts with `phar://`, an exception is raised. However, PHP wrappers being case insensitive, this patch can be bypassed using `PHAR://` instead of `phar://`. A successful exploitation of this vulnerability allows executing arbitrary code and accessing the underlying filesystem. The attacker must be able to upload a file and the server must be running a PHP version prior to 8. This issue has been addressed in commit `d3b742d61a` which has been included in version 1.4.3. Users are advised to upgrade. Users unable to upgrade should ensure that only trusted users may submit data to the `AbstractGenerator->generate(...)` function.

References

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

Affected Components

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

Weakness

CWE-502

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2023-37460

Description

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

References

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

Affected Components

Component	Artifact Id	Version
Plexus Archiver Component	plexus-archiver-3.4.jar	3.4

Weakness

CWE-22

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.36 % 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-2023-28115

Doc. Identifier: \${document.id}

Description

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

References

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

Affected Components

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

Weakness

CWE-502

Initial Severity

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

Advisories

Alerts

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

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

CVE-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-1.5.jar	1.5

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



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2021-36374

Description

When reading a specially crafted ZIP archive, or a derived formats, an Apache Ant build can be made to allocate large amounts of memory that leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Commonly used derived formats from ZIP archives are for instance JAR files and many office files. Apache Ant prior to 1.9.16 and 1.10.11 were affected.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-36374

Affected Components

Component	Artifact Id	Version
Apache Ant Launcher	ant-launcher-1.10.1.jar	1.10.1
	ant-1.10.1.jar	1.10.1

Weakness

CWE-130

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-5v34-g2px-j4fw	Improper Handling of Length Parameter Inconsistency in Apache Ant	2021-08-02	2021-08-02

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/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 66.13 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-36373

Description

When reading a specially crafted TAR archive an Apache Ant build can be made to allocate large amounts of memory that finally leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Apache Ant prior to 1.9.16 and 1.10.11 were affected.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-36373

Affected Components

Component	Artifact Id	Version
Apache Ant Launcher	ant-launcher-1.10.1.jar	1.10.1
	ant-1.10.1.jar	1.10.1

Weakness

CWE-130

Initial Severity

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

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-q5r4-cfpx-h6fh	Improper Handling of Length Parameter Inconsistency in Apache Ant	2021-08-02	2021-08-02

Assessment

Summary

Incignificant	Dofault	Modium
Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.11 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 54.76 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is insignificant .

CVE-2021-36090

Description

When reading a specially crafted ZIP archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' zip package.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-36090

Affected Components

Component	Artifact Id	Version
Apache Commons Compress	commons-compress-1.11.jar	1.11

Weakness

CWE-130

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-mc84-pj99-q6hh	Improper Handling of Length Parameter Inconsistency in Compress	2021-08-02	2021-08-02

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS: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 1.37 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 13.20 % 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-2021-35517

Description

When reading a specially crafted TAR archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' tar package.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-35517

Affected Components

Component	Artifact Id	Version
Apache Commons Compress	commons-compress-1.11.jar	1.11

Weakness

CWE-130, CWE-770

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-xqfj-vm6h-2x34	Improper Handling of Length Parameter Inconsistency in Compress	2021-08-02	2021-08-02

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

Doc. Identifier: \${document.id}

\${document.name} Page 18 of 64 Doc. Version: \${document.versic Doc. Date: \${document.date_

Criteria	Explanation
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 13.29 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2021-35516

Description

When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-35516

Affected Components

Component	Artifact Id	Version
Apache Commons Compress	commons-compress-1.11.jar	1.11

Weakness

CWE-130, CWE-770

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-crv7-7245-f45f	Improper Handling of Length Parameter Inconsistency in Compress	2021-08-02	2021-08-02

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.50 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 9.51 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2021-35515

Description

When reading a specially crafted 7Z archive, the construction of the list of codecs that decompress an entry can result in an infinite loop. This could be used to mount a denial of service attack against services that use Compress' sevenz package.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-35515

Affected Components

Component	Artifact Id	Version
Apache Commons Compress	commons-compress-1.11.jar	1.11

Weakness

CWE-834, CWE-835

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-7hfm-57qf-j43q	Excessive Iteration in Compress	2021-08-02	2021-08-02

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS: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 2.13 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 10.37 % 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-2021-34083

Description

Google-it is a Node.js package which allows its users to send search queries to Google and receive the results in a JSON format. When using the 'Open in browser' option in versions up to 1.6.2, google-it will unsafely concat the result's link retrieved from google to a shell command, potentially exposing the server to RCE.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-34083

Affected Components

Component	Artifact Id	Version
Google Collections Library	google-collections-1.0.jar	1.0

Weakness

CWE-78

Initial Severity

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

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-7xhv-mpjw-422f	Command injection in google-it	2022-06-03	2022-06-03

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 1.94 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 10.87 % 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-2021-29425

Description

In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "//../foo", or "\...\foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-29425

Affected Components

Component	Artifact Id	Version
Apache Commons IO	commons-io-2.5.jar	2.5

Weakness

CWE-20, CWE-22

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	4.8	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	5.8	AV:N/AC:M/Au:N/C:P/I:P/A:N	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-gwrp-pvrq-jmwv	Path Traversal and Improper Input Validation in Apache Commons IO	2021-04-26	2021-04-26

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Doc. Identifier: \${document.id}

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/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 42.37 % 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 insignificant .

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
Maven Compat	maven-compat-3.0.5.jar	3.0.5
Maven Settings Builder	maven-settings-builder-3.0.5.jar	3.0.5
Apache Maven Wagon :: API	wagon-provider-api-2.4.jar	2.4
Maven Model Builder	maven-model-builder-3.0.5.jar	3.0.5
Maven Aether Provider	maven-aether-provider-3.0.5.jar	3.0.5
Maven Core	maven-core-3.0.5.jar	3.0.5
Maven Plugin API	maven-plugin-api-3.0.5.jar	3.0.5
Maven Settings	maven-settings-3.3.9.jar	3.3.9
Maven Model	maven-model-3.0.5.jar	3.0.5
Maven Repository Metadata Model	maven-repository-metadata-3.0.5.jar	3.0.5
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

Weakness

CWE-346

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	Critical
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N	Medium

Advisories

Alerts

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

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2020-8927

Description

A buffer overflow exists in the Brotli library versions prior to 1.0.8 where an attacker controlling the input length of a "one-shot" decompression request to a script can trigger a crash, which happens when copying over chunks of data larger than 2 GiB. It is recommended to update your Brotli library to 1.0.8 or later. If one cannot update, we recommend to use the "streaming" API as opposed to the "one-shot" API, and impose chunk size limits.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-8927

Affected Components

Component	Artifact Id	Version
Google Collections Library	google-collections-1.0.jar	1.0

Weakness

CWE-130, CWE-120

Initial Severity

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

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L	Medium
CVSS:2.0	NVD-CNA-NVD	6.4	AV:N/AC:L/Au:N/C:N/I:P/A:P	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-5v8v-66v8-mwm7	Integer overflow in the bundled Brotli C library	2022-05-24	2022-05-24

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation	
CVSS Overall	CVSS:4.0 GitHub, Inc. provides the vector: CVSS:4.0 /AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N	
Keywords	No keyword sets matched.	
EPSS	This vulnerability has a 0.95 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 16.17 % of all scored vulnerabilities.	
KEV	This vulnerability has not been confirmed to have been exploited in the wild.	
EOL	No end-of-life (EOL) information available.	
Assessment	The vulnerability status is insignificant .	

CVE-2020-1945

Description

Apache Ant 1.1 to 1.9.14 and 1.10.0 to 1.10.7 uses the default temporary directory identified by the Java system property java.io.tmpdir for several tasks and may thus leak sensitive information. The fixcrlf and replaceregexp tasks also copy files from the temporary directory back into the build tree allowing an attacker to inject modified source files into the build process.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-1945

Affected Components

Component	Artifact Id	Version
Apache Ant Launcher	ant-launcher-1.10.1.jar	1.10.1
	ant-1.10.1.jar	1.10.1

Weakness

CWE-668

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.3	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	3.3	AV:L/AC:M/Au:N/C:P/I:P/A:N	Low

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-4p6w-m9wc-c9c9	Sensitive Data Exposure in Apache Ant	2020-09-14	2020-09-14

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation	
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N	
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 65.52 % of all scored vulnerabilities.	
KEV	This vulnerability has not been confirmed to have been exploited in the wild.	
EOL	No end-of-life (EOL) information available.	
Assessment	The vulnerability status is insignificant .	

CVE-2020-13936

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	velocity-1.7.jar	1.7

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	High
CVSS:2.0	NVD-CNA-NVD	9.0	AV:N/AC:L/Au:S/C:C/I:C/A:C	Critical

Advisories

Alerts

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

Assessment

Summary



CVSS Vector Severity Charts

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.

Criteria	Explanation
EPSS	This vulnerability has a 0.17 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 44.92 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2020-10683

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	dom4j-1.6.1.jar	1.6.1

Weakness

CWE-611

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary



CVSS Vector Severity Charts

Doc. Identifier: \${document.id}

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2018-15756

Description

Spring Framework, version 5.1, versions 5.0.x prior to 5.0.10, versions 4.3.x prior to 4.3.20, and older unsupported versions on the 4.2.x branch provide support for range requests when serving static resources through the ResourceHttpRequestHandler, or starting in 5.0 when an annotated controller returns an org.springframework.core.io.Resource. A malicious user (or attacker) can add a range header with a high number of ranges, or with wide ranges that overlap, or both, for a denial of service attack. This vulnerability affects applications that depend on either spring-webmvc or spring-webflux. Such applications must also have a registration for serving static resources (e.g. JS, CSS, images, and others), or have an annotated controller that returns an org.springframework.core.io.Resource. Spring Boot applications that depend on spring-boot-starter-web or spring-boot-starter-webflux are ready to serve static resources out of the box and are therefore vulnerable.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-15756

Affected Components

Doc. Identifier: \${document.id}

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-ffvq-7w96-97p7	Denial of Service in Spring Framework	2020-06-15	2020-06-15

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 GitHub, Inc. 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 0.45 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 24.20 % 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-2018-1324

Description

A specially crafted ZIP archive can be used to cause an infinite loop inside of Apache Commons Compress' extra field parser used by the ZipFile and ZipArchiveInputStream classes in versions 1.11 to 1.15. This can be used to mount a denial of service attack against services that use Compress' zip package.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1324

Affected Components

Doc. Identifier: \${document.id}

Component	Artifact Id	Version
Apache Commons Compress	commons-compress-1.11.jar	1.11

Weakness

CWE-835

\$\{\text{document.name}\} \text{Doc. Version: \$\{\text{document.versi}\}} \text{Page 31 of 64} \text{Doc. Date: \$\{\text{document.date}\}}

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-h436-432x-8fvx	Apache Commons Compress vulnerable to denial of service due to infinite loop	2019-03-14	2019-03-14

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.13 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 50.67 % 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-2018-1275

Doc. Identifier: \${document.id}

Description

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.16 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack. This CVE addresses the partial fix for CVE-2018-1270 in the 4.3.x branch of the Spring Framework.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1275

Affected Components

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

Weakness

CWE-94, CWE-358

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-3rmv-2pg5-xvqj	Improperly Implemented Security Check for Standard in org.springframework:spring-core	2018-10-17	2018-10-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 18.16 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 3.66 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

Doc. Identifier: \${document.id}

\${document.name} Doc. Version: \${document.versi} Page 33 of 64 Doc. Date: \${document.date_

CVE-2018-1272

Description

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, provide client-side support for multipart requests. When Spring MVC or Spring WebFlux server application (server A) receives input from a remote client, and then uses that input to make a multipart request to another server (server B), it can be exposed to an attack, where an extra multipart is inserted in the content of the request from server A, causing server B to use the wrong value for a part it expects. This could to lead privilege escalation, for example, if the part content represents a username or user roles.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1272

Affected Components

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	High
CVSS:2.0	NVD-CNA-NVD	6.0	AV:N/AC:M/Au:S/C:P/I:P/A:P	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-4487-x383-qpph	Possible privilege escalation in org.springframework:spring-core	2018-10-17	2018-10-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

Doc. Identifier: \${document.id}

\${document.name} Page 34 of 64 Doc. Version: \${document.version Doc. Date: \${document.date_

Criteria	Explanation
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 42.57 % 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-2018-1271

Description

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, allow applications to configure Spring MVC to serve static resources (e.g. CSS, JS, images). When static resources are served from a file system on Windows (as opposed to the classpath, or the ServletContext), a malicious user can send a request using a specially crafted URL that can lead a directory traversal attack.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1271

Affected Components

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

Weakness

CWE-22

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	Medium
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-g8hw-794c-4j9g	Path Traversal in org.springframework:spring-core	2018-10-17	2018-10-17

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/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 26.60 % 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-2018-1270

Description

Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1270

Affected Components

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

Weakness

CWE-94, CWE-358

Doc. Identifier: \${document.id}

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-p5hg-3xm3-gcjg	Spring Framework allows applications to expose STOMP over WebSocket endpoints	2018-10-17	2018-10-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (11.1 from base score 9.8)

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 76.79 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 1.70 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2018-1257

Description

Spring Framework, versions 5.0.x prior to 5.0.6, versions 4.3.x prior to 4.3.17, and older unsupported versions allows applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a regular expression, denial of service attack.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1257

Affected Components

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

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
CVSS:2.0	NVD-CNA-NVD	4.0	AV:N/AC:L/Au:S/C:N/I:N/A:P	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-rcpf-vj53-7h2m	Denial of Service in org.springframework:spring-core	2018-10-17	2018-10-17

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV: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 0.17 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 44.97 % 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-2018-1199

Description

Spring Security (Spring Security 4.1.x before 4.1.5, 4.2.x before 4.2.4, and 5.0.x before 5.0.1; and Spring Framework 4.3.x before 4.3.14 and 5.0.x before 5.0.3) does not consider URL path parameters when processing security constraints. By adding a URL path parameter with special encodings, an attacker may be able to bypass a security constraint. The root cause of this issue is a lack of clarity regarding the handling of path parameters in the Servlet Specification. Some Servlet containers include path parameters in the value returned for getPathInfo() and some do not. Spring Security uses the value returned by getPathInfo() as part of the process of mapping requests to security constraints. In this particular attack, different character encodings used in path parameters allows secured Spring MVC static resource URLs to be bypassed.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1199

Affected Components

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

Weakness

CWE-20

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-v596-fwhq-8x48	Improper Input Validation in org.springframework.security:spring-security-core, org.springframework.security:spring-security-core, and org.springframework:spring-core	2018-10-17	2018-10-17

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV: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 0.18 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 43.86 % 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.

Criteria	Explanation
Assessment	The vulnerability status is insignificant .

CVE-2018-11771

Description

When reading a specially crafted ZIP archive, the read method of Apache Commons Compress 1.7 to 1.17's ZipArchiveInputStream can fail to return the correct EOF indication after the end of the stream has been reached. When combined with a java.io.InputStreamReader this can lead to an infinite stream, which can be used to mount a denial of service attack against services that use Compress' zip package.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-11771

Affected Components

Component	Artifact Id	Version
Apache Commons Compress	commons-compress-1.11.jar	1.11

Weakness

CWE-835

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-hrmr-f5m6-m9pq	Moderate severity vulnerability that affects org.apache.commons:commons-compress	2018-10-19	2018-10-19

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Doc. Identifier: \${document.id}

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.15 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 48.22 % 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 insignificant .

CVE-2018-11040

Description

Spring Framework, versions 5.0.x prior to 5.0.7 and 4.3.x prior to 4.3.18 and older unsupported versions, allows web applications to enable cross-domain requests via JSONP (JSON with Padding) through AbstractJsonpResponseBodyAdvice for REST controllers and MappingJackson2JsonView for browser requests. Both are not enabled by default in Spring Framework nor Spring Boot, however, when MappingJackson2JsonView is configured in an application, JSONP support is automatically ready to use through the "jsonp" and "callback" JSONP parameters, enabling cross-domain requests.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-11040

Affected Components

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

Weakness

CWE-829

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	High
CVSS:2.0	NVD-CNA-NVD	4.3	AV:N/AC:M/Au:N/C:P/I:N/A:N	Medium

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-f26x-pr96-vw86	Moderate severity vulnerability that affects org.springframework:springcore	2018-10-16	2018-10-16

Doc. Identifier: \${document.id} \${document.name} Doc. Version: \${document.versi} Page 41 of 64 Doc. Date: \${document.date_

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.25 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 34.71 % 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-2018-1002200

Description

plexus-archiver before 3.6.0 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in an archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2018-1002200

Affected Components

Component	Artifact Id	Version
Plexus Archiver Component	plexus-archiver-3.4.jar	3.4

Weakness

CWE-22

Initial Severity

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-hcxq-x77q-3469	Improper Limitation of a Pathname to a Restricted Directory in plexus-archiver	2022-05-13	2022-05-13

Assessment

Summary

Insignificant	Default	Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

	•
Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.13 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 51.19 % 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-2018-1000632

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	dom4j-1.6.1.jar	1.6.1

Weakness

CWE-91

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2015-7501

Doc. Identifier: \${document.id}

Description

Red Hat JBoss A-MQ 6.x; BPM Suite (BPMS) 6.x; BRMS 6.x and 5.x; Data Grid (JDG) 6.x; Data Virtualization (JDV) 6.x and 5.x; Enterprise Application Platform 6.x, 5.x, and 4.3.x; Fuse 6.x; Fuse Service Works (FSW) 6.x; Operations Network (JBoss ON) 3.x; Portal 6.x; SOA Platform (SOA-P) 5.x; Web Server (JWS) 3.x; Red Hat OpenShift/xPAAS 3.x; and Red Hat Subscription Asset Manager 1.3 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2015-7501

Affected Components

Component	Artifact Id	Version
Commons Collections	commons-collections-3.2.1.jar	3.2.1

Weakness

CWE-502

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Critical
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-fjq5-5j5f-mvxh	Deserialization of Untrusted Data in Apache commons collections	2022-05-13	2022-05-13

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 2.47 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 9.57 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2015-6420

Description

Serialized-object interfaces in certain Cisco Collaboration and Social Media; Endpoint Clients and Client Software; Network Application, Service, and Acceleration; Network and Content Security Devices; Network Management and Provisioning; Routing and Switching - Enterprise and Service Provider; Unified Computing; Voice and Unified Communications Devices; Video, Streaming, TelePresence, and Transcoding Devices; Wireless; and Cisco Hosted Services products allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2015-6420

Affected Components

Component	Artifact Id	Version
Commons Collections	commons-collections-3.2.1.jar	3.2.1

Weakness

CWE-502

Initial Severity

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

Advisories

Alerts

ld	Summary	Create Date	Update Date
GHSA-6hgm-866r-3cjv	Insecure Deserialization in Apache Commons Collection	2020-06-15	2020-06-15

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS: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 0.88 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 16.88 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

CVE-2015-4035

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-1.5.jar	1.5

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

Doc. Identifier: \${document.id}

Alerts

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

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2012-5817

Description

Codehaus XFire 1.2.6 and earlier, as used in the Amazon EC2 API Tools Java library and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2012-5817

Affected Components

Component	Artifact Id	Version
jaxen	jaxen-1.1.6.jar	1.1.6

Weakness

CWE-295

Initial Severity

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

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-5jc8-8xhv-g8qm	Improper Input Validation in XFire	2022-05-17	2022-05-17

Assessment

Summary



CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a 0.11 % chance of being exploited in the next 30 days according to FIRST. It ranks in the top 53.55 % of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is in review .

4 ae-dita Affected Components

Google Collections Library

Artifacts

Component	Artifact Id	Version
Google Collections Library	google-collections-1.0.jar	1.0

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-34083	8.1		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-7xhv-mpjw-422f cpe:/a:google-it_project:google-it:::~~~node.js~~ [, 1.6.2]					
CVE-2020-8927	6.9		Medium		Default	Insignificant
	GHSA-5v8v-66v8-mwm7					
	cpe:/a:google:brotli [, 1.0.8)					

Table 1: Google Collections Library Vulnerabilities

Commons Collections

Artifacts

Component	Artifact Id	Version
Commons Collections	commons-collections-3.2.1.jar	3.2.1

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2015-7501	9.8		Critical		Default	In Review	
	GHSA-fjq5-5j5f-mvxh						
	GHSA commons-collections:commons-collections (Maven) [0, 3.2.2)						
CVE-2015-6420	7.5		High		Default	In Review	
	GHSA-6hgm-866r-3cjv						
	cpe:/a:apache:commons_collections [, 3.2.1], GHSA commons-collections:commons-collections (Maven) [0, 3. 2.2)						

Table 2: Commons Collections Vulnerabilities

Apache Commons IO

Artifacts

Component	Artifact Id	Version
Apache Commons IO	commons-io-2.5.jar	2.5

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-47554	8.7		High		Default	In Review
	GHSA-78wr-2p64	-hpwj				
	GHSA commons-io:commons-io (Maven) [2.0, 2.14.0)					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-29425	4.8		Medium		Default	Insignificant	
	GHSA-gwrp-pvrq-jmwv						
	cpe:/a:apache:commons_io:2.5:- 2.5 (-), GHSA commons-io:commons-io (Maven) [0, 2.7)						

Table 3: Apache Commons IO Vulnerabilities

jaxen

Artifacts

Component	Artifact Id	Version
jaxen	jaxen-1.1.6.jar	1.1.6

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2012-5817	7.4		High		Default	In Review	
	GHSA-5jc8-8xhv-g8qm						
	cpe:/a:codehaus:	dire [, 1.2.6]					

Table 4: jaxen Vulnerabilities

Apache Ant Launcher

Artifacts

Component	Artifact Id	Version
Apache Ant Launcher	ant-launcher-1.10.1.jar	1.10.1

Vulnerabilities

Doc. Identifier: \${document.id}

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2021-36374	5.5		Medium		Default	Insignificant		
	GHSA-5v34-g2px	GHSA-5v34-g2px-j4fw						
	cpe:/a:apache:ant	[1.10.0, 1.10.11),	GHSA org.apach	ne.ant:ant (Mave	n) [1.10.0, 1.10.11)			
CVE-2021-36373	5.5		Medium		Default	Insignificant		
	GHSA-q5r4-cfpx-h	n6fh						
	cpe:/a:apache:ant	[1.10.0, 1.10.11),	GHSA org.apach	ne.ant:ant (Mave	n) [1.10.0, 1.10.11)			
CVE-2020-1945	6.3		Medium		Default	Insignificant		
	GHSA-4p6w-m9wc-c9c9							

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:apache:ant [1.10.0, 1.10.7], GHSA org.apache.ant:ant (Maven) [1.10.0, 1.10.8)					

Table 5: Apache Ant Launcher Vulnerabilities

Apache Commons Compress

Artifacts

Component	Artifact Id	Version
Apache Commons Compress	commons-compress-1.11.jar	1.11

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2024-25710	5.5		Medium		Default	Insignificant	
	GHSA-4g9r-vxhx-	9pgx					
	cpe:/a:apache:commons_compress [1.3, 1.26.0), GHSA org.apache.commons:commons-compress (M [1.3, 1.26.0)						
CVE-2021-36090	7.5		High		Default	In Review	
	GHSA-mc84-pj99	-q6hh					
	cpe:/a:apache:cor 1.21)	mmons_compress	[1.0, 1.21), GHS	A org.apache.co	mmons:commons-	compress (Maven) [0,	
CVE-2021-35517	7.5		High		Default	In Review	
	GHSA-xqfj-vm6h-	2x34					
	cpe:/a:apache:cor 1.21)	mmons_compress	[1.1, 1.20], GHS	A org.apache.co	mmons:commons-	compress (Maven) [0,	
CVE-2021-35516	7.5		High		Default	In Review	
	GHSA-crv7-7245-	f45f					
	cpe:/a:apache:cor 1.21)	mmons_compress	[1.6, 1.20], GHS.	A org.apache.co	mmons:commons-	compress (Maven) [0,	
CVE-2021-35515	7.5		High		Default	In Review	
	GHSA-7hfm-57qf-j43q						
	cpe:/a:apache:cor 1.21)	mmons_compress	[1.6, 1.20], GHS.	A org.apache.co	mmons:commons-	compress (Maven) [0,	
CVE-2018-1324	5.5		Medium		Default	Insignificant	
	GHSA-h436-432x	-8fvx					
	cpe:/a:apache:cor [1.11, 1.16)	mmons_compress	[1.11, 1.15], GHS	SA org.apache.c	ommons:commons	-compress (Maven)	
CVE-2018-11771	5.5		Medium		Default	Insignificant	

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
	GHSA-hrmr-f5m6-m9pq						
	cpe:/a:apache:commons_compress [1.7.0, 1.17.0], GHSA org.apache.commons:commons-compress (Maven) [1.7, 1.18)						

Table 6: Apache Commons Compress Vulnerabilities

Maven Plugin Tools Java 5 Annotations

Artifacts

Component	Artifact Id	Version
Maven Plugin Tools Java 5 Annotations	maven-plugin-annotations-3.5.jar	3.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
GHSA-2f88-5hg8-9x2x							
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 7: Maven Plugin Tools Java 5 Annotations 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 8: 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 9: 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 10: Maven Artifact Vulnerabilities

Maven Compat

Artifacts

Component	Artifact Id	Version
Maven Compat	maven-compat-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2021-26291	9.1		Critical		Default	In Review	
	GHSA-2f88-5hg8-9x2x						
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)						

Table 11: Maven Compat Vulnerabilities

Doc. Identifier: \${document.id}

Maven Core

Artifacts

Component	Artifact Id	Version
Maven Core	maven-core-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)					.1), GHSA org.

Table 12: Maven Core Vulnerabilities

Maven Model Builder

Artifacts

Component	Artifact Id	Version
Maven Model Builder	maven-model-builder-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven-compat (Maven) [0, 3.8.1)					s.1), GHSA org.	

Table 13: Maven Model Builder Vulnerabilities

Maven Model

Artifacts

Component	Artifact Id	Version
Maven Model	maven-model-3.0.5.jar	3.0.5

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-	-9x2x				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)					

Table 14: Maven Model Vulnerabilities

Maven Plugin API

Artifacts

Component	Artifact Id	Version
Maven Plugin API	maven-plugin-api-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					
						3.1), GHSA org.

Table 15: Maven Plugin API Vulnerabilities

Maven Repository Metadata Model

Artifacts

Component	Artifact Id	Version
Maven Repository Metadata Model	maven-repository-metadata-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)					.1), GHSA org.

Table 16: Maven Repository Metadata Model Vulnerabilities

Maven Settings Builder

Artifacts

Component	Artifact Id	Version
Maven Settings Builder	maven-settings-builder-3.0.5.jar	3.0.5

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)					3.1), GHSA org.

Table 17: Maven Settings Builder Vulnerabilities

Maven Settings

Artifacts

Component	Artifact Id	Version
Maven Settings	maven-settings-3.3.9.jar	3.3.9

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org. apache.maven:maven-core (Maven) [0, 3.8.1)					3.1), GHSA org.

Table 18: Maven Settings Vulnerabilities

Plexus Archiver Component

Artifacts

Component	Artifact Id	Version
Plexus Archiver Component	plexus-archiver-3.4.jar	3.4

Vulnerabilities

Doc. Identifier: \${document.id}

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2023-37460	9.8		Critical		Default	In Review
	GHSA-wh3p-fphp-9h2m					
	cpe:/a:codehaus-plexus:plexus-archiver [, 4.8.0), GHSA org.codehaus.plexus:plexus-archiver [)					hiver (Maven) [0, 4.8.
CVE-2018-1002200	5.5		Medium		Default	Insignificant
	GHSA-hcxq-x77q-3469					

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	cpe:/a:codehaus- 0)	olexus:plexus-archi	iver [, 3.6.0), GH	SA org.codehau	s.plexus:plexus-arc	chiver (Maven) [0, 3.6.

Table 19: Plexus Archiver Component Vulnerabilities

snappy

Artifacts

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

Vulnerabilities

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2024-36124	5.3		Medium		Default	Insignificant
	GHSA-8wh2-6qhj-	-h7j9				
	GHSA org.iq80.sn	appy:snappy (Mav	ren) [0, 0.5)			
CVE-2023-41330	9.8		Critical		Default	In Review
	GHSA-92rv-4j2h-8	Bmjj				
	cpe:/a:knplabs:sna	арру [, 1.4.3)				
CVE-2023-28115	9.8		Critical		Default	In Review
	GHSA-gq6w-q6wh-jggc					
	cpe:/a:knplabs:sna	арру [, 1.4.2)				

Table 20: snappy Vulnerabilities

Spring Core

Artifacts

Component	Artifact Id	Version
Spring Core	spring-core-4.3.10.RELEASE.jar	4.3.10.RELEASE

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
CVE-2018-15756	7.5		High		Default	In Review
	GHSA-ffvq-7w96-97p7					
	GHSA org.springframework:spring-core (Maven) [4.2.0.RELEASE, 4.3.20.RELEASE)					
CVE-2018-1275	9.8		Critical		Default	In Review

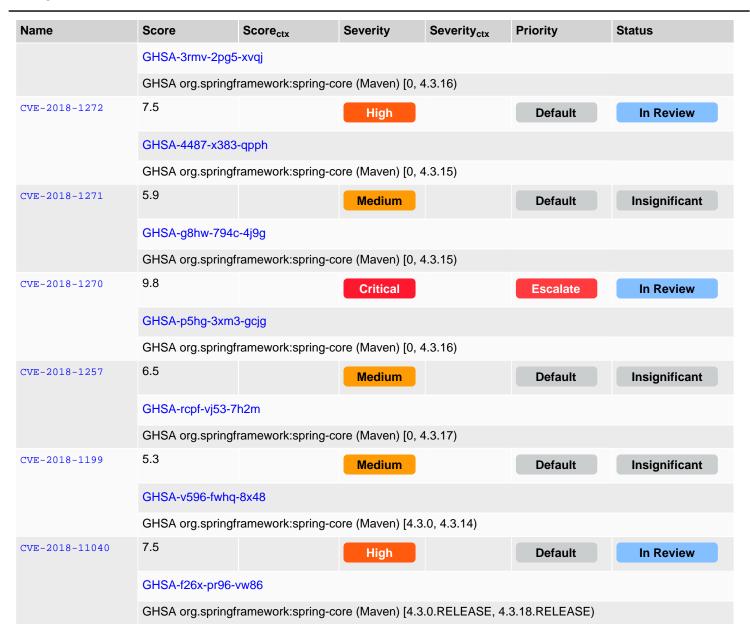


Table 21: Spring Core Vulnerabilities

XZ for Java

Artifacts

Component	Artifact Id	Version
XZ for Java	xz-1.5.jar	1.5

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2022-1271	8.8		High		Default	In Review		
	GHSA-jrpw-543v	GHSA-jrpw-543v-8r62						
	cpe:/a:tukaani:xz	cpe:/a:tukaani:xz [, 5.2.5)						

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status	
CVE-2015-4035	7.8		High		Default	In Review	
	GHSA-mf33-8p24-6h53						
	cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]						

Table 22: XZ for Java Vulnerabilities

5 ae-dita Vulnerability Notice

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

6 ae-dita Vulnerability List

The following vulnerabilities have been identified and categorized.

Applicable

No vulnerabilities are considered Applicable within the given configuration.

In Review

The following vulnerabilities are considered In Review within the given configuration:

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status		
CVE-2023-41330	9.8		Critical		Default	In Review		
	GHSA-92rv-4j2h-8mjj							
	cpe:/a:knplabs:sn	арру [, 1.4.3)						
CVE-2023-37460	9.8		Critical		Default	In Review		
	GHSA-wh3p-fphp	-9h2m						
	cpe:/a:codehaus-plexus:plexus-archiver [, 4.8.0), GHSA org.codehaus.plexus:plexus-archiver (Maven) [0, 4.8.0)							
CVE-2023-28115	9.8		Critical		Default	In Review		
	GHSA-gq6w-q6w	h-jggc						
	cpe:/a:knplabs:sn	арру [, 1.4.2)						
CVE-2020-10683	9.8		Critical		Default	In Review		
	GHSA-hwj3-m3p6-hj38							
	cpe:/a:dom4j_proj	ect:dom4j [, 2.0.3)	, GHSA org.dom	4j:dom4j (Maver) [0, 2.0.3)			
CVE-2018-1275	9.8		Critical		Default	In Review		

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-3rmv-2pg5	-xvqj				
	GHSA org.springf	ramework:spring-c	ore (Maven) [0,	4.3.16)		
CVE-2018-1270	9.8		Critical		Escalate	In Review
	GHSA-p5hg-3xm3	B-gcjg				
	GHSA org.springf	ramework:spring-c	ore (Maven) [0, 4	4.3.16)		
CVE-2015-7501	9.8		Critical		Default	In Review
	GHSA-fjq5-5j5f-m	vxh				
	GHSA commons-	collections:commo	ns-collections (M	laven) [0, 3.2.2)		
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-	9x2x				
		ven [, 3.8.1), GHS/ aven-core (Maven)		aven:maven-con	npat (Maven) [0, 3.8	8.1), GHSA org.
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	e.velocity:velocity (Maven) [0, 1.7]			
CVE-2024-47554	8.7		High		Default	In Review
	GHSA-78wr-2p64	-hpwj				
	GHSA commons-	o:commons-io (Ma	aven) [2.0, 2.14.0))		
CVE-2021-34083	8.1		High		Default	In Review
	GHSA-7xhv-mpjw	-422f				
	cpe:/a:google-it_p	roject:google-it:::~	~~node.js~~ [, 1.	6.2]		
CVE-2015-4035	7.8		High		Default	In Review
	GHSA-mf33-8p24	-6h53				
	cpe:/a:tukaani:xz:	beta * (beta)[, 4.99	99.9]			
CVE-2021-36090	7.5		High		Default	In Review
	GHSA-mc84-pj99	-q6hh				
	cpe:/a:apache:cor	mmons_compress	[1.0, 1.21), GHS	A org.apache.co	ommons:commons-	compress (Maven) [0,
CVE-2021-35517	7.5		High		Default	In Review

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA-xqfj-vm6	h-2x34				
	cpe:/a:apache:c	commons_compre	ess [1.1, 1.20], GH	SA org.apache.c	ommons:common	ns-compress (Maven) [0
CVE-2021-35516	7.5		High		Default	In Review
	GHSA-crv7-724	15-f45f				
	cpe:/a:apache:c	commons_compre	ess [1.6, 1.20], GH	SA org.apache.c	ommons:common	ns-compress (Maven) [0
CVE-2021-35515	7.5		High		Default	In Review
	GHSA-7hfm-57	qf-j43q				
	cpe:/a:apache:c	commons_compre	ess [1.6, 1.20], GH	SA org.apache.c	ommons:common	ns-compress (Maven) [0
CVE-2018-15756	7.5		High		Default	In Review
	GHSA-ffvq-7w9	6-97p7				
	GHSA org.sprin	gframework:sprin	g-core (Maven) [4	.2.0.RELEASE, 4	1.3.20.RELEASE)	
CVE-2018-1272	7.5		High		Default	In Review
	GHSA-4487-x3	83-qpph				
	GHSA org.sprin	gframework:sprin	g-core (Maven) [0	, 4.3.15)		
CVE-2018-11040	7.5		High		Default	In Review
	GHSA-f26x-pr9	6-vw86				
	GHSA org.sprin	gframework:sprin	g-core (Maven) [4	.3.0.RELEASE, 4	1.3.18.RELEASE)	
CVE-2018-1000632	7.5		High		Default	In Review
	GHSA-6pcc-3rfz	x-4gpm				
	GHSA org.dom	4j:dom4j (Maven)	[0, 2.0.3)			
CVE-2015-6420	7.5		High		Default	In Review
	GHSA-6hgm-86	66r-3cjv				
	cpe:/a:apache:c	commons_collecti	ons [, 3.2.1], GHS	A commons-colle	ections:commons-	collections (Maven) [0, 3
CVE-2012-5817	7.4		High		Default	In Review
	GHSA-5jc8-8xh	v-g8qm				
	cpe:/a:codehau	s:xfire [, 1.2.6]				
CVE-2023-45960					Default	In Review
	GHSA-fgq9-fc3	q-vqmw				

Name	Score	Score _{ctx}	Severity	Severity _{ctx}	Priority	Status
	GHSA org.dom4j:dom4j (Maven) [0, 2.1.4]					

Table 23: In Review Category (ae-dita)

Not Applicable

No vulnerabilities are considered ${\tt Not}\,$ 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-2020-8927	6.9		Medium		Default	Insignificant		
	GHSA-5v8v-66v8-mwm7							
	cpe:/a:google:brot	li [, 1.0.8)						
CVE-2018-1257	6.5		Medium		Default	Insignificant		
	GHSA-rcpf-vj53-7h2m							
	GHSA org.springf	ramework:spring-co	ore (Maven) [0, 4	l.3.17)				
CVE-2020-1945	6.3		Medium		Default	Insignificant		
	GHSA-4p6w-m9w	rc-c9c9						
	cpe:/a:apache:ant	[1.10.0, 1.10.7], G	HSA org.apache	.ant:ant (Maven) [1.10.0, 1.10.8)			
CVE-2018-1271	5.9		Medium		Default	Insignificant		
	GHSA-g8hw-794c-4j9g							
	GHSA org.springf	ramework:spring-co	ore (Maven) [0, 4	l.3.15)				
CVE-2024-25710	5.5		Medium		Default	Insignificant		
	GHSA-4g9r-vxhx-	9pgx						
	cpe:/a:apache:cor [1.3, 1.26.0)	nmons_compress	[1.3, 1.26.0), GH	SA org.apache.o	commons:commons	s-compress (Maven)		
CVE-2021-36374	5.5		Medium		Default	Insignificant		
	GHSA-5v34-g2px	-j4fw						
	cpe:/a:apache:ant	[1.10.0, 1.10.11),	GHSA org.apach	e.ant:ant (Mave	n) [1.10.0, 1.10.11)			
CVE-2021-36373	5.5		Medium		Default	Insignificant		
	GHSA-q5r4-cfpx-h6fh							
	cpe:/a:apache:ant	[1.10.0, 1.10.11),	GHSA org.apach	e.ant:ant (Mave	n) [1.10.0, 1.10.11)			
CVE-2018-1324	5.5		Medium		Default	Insignificant		

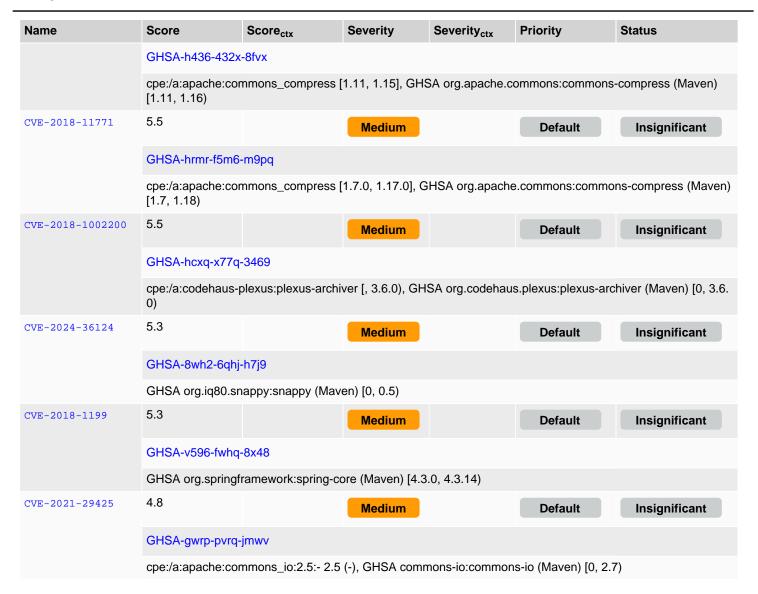


Table 24: Insignificant Category (ae-dita)

Void

Doc. Identifier: \${document.id}

No vulnerabilities are considered void within the given configuration.