

\${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

2 ae-dita Affected Assets.....

4

3 ae-dita Vulnerability Details.....

4

CVE-2024-47554.....

4

CVE-2024-36124.....

5

CVE-2024-25710.....

7

CVE-2023-45960.....

8

CVE-2023-41330.....

9

CVE-2023-37460.....

10

CVE-2023-28115.....

11

CVE-2022-1271.....

13

CVE-2021-36374.....

14

CVE-2021-36373.....

15

CVE-2021-36090.....

16

CVE-2021-35517.....

18

CVE-2021-35516.....

19

CVE-2021-35515.....

20

CVE-2021-34083.....

21

CVE-2021-29425.....

22

CVE-2021-26291.....

24

CVE-2020-8927.....

25

CVE-2020-1945.....

26

CVE-2020-13936.....

28

CVE-2020-10683.....

29

CVE-2018-15756.....

30

CVE-2018-1324.....

31

CVE-2018-1275.....

32

CVE-2018-1272.....

34

CVE-2018-1271.....

35

CVE-2018-1270.....

36

CVE-2018-1257.....

37

CVE-2018-1199.....

38

CVE-2018-11771.....

40

CVE-2018-11040.....

41

CVE-2018-1002200.....

42

CVE-2018-1000632.....

43

CVE-2015-7501.....

44

CVE-2015-6420.....

46

CVE-2015-4035.....

47

CVE-2012-5817.....

48

4 ae-dita Affected Components.....

49

Google Collections Library.....

49

Commons Collections.....

50

Apache Commons IO.....

50

jaxen.....

51

Apache Ant Launcher.....

51

Apache Commons Compress.....	52
Maven Plugin Tools Java 5 Annotations.....	53
Apache Maven Wagon :: API.....	53
Maven Aether Provider.....	53
Maven Artifact.....	54
Maven Compat.....	54
Maven Core.....	55
Maven Model Builder.....	55
Maven Model.....	55
Maven Plugin API.....	56
Maven Repository Metadata Model.....	56
Maven Settings Builder.....	56
Maven Settings.....	57
Plexus Archiver Component.....	57
snappy.....	58
Spring Core.....	58
XZ for Java.....	59

**5 ae-dita Vulnerability Notice.....60**

6 ae-dita Vulnerability List..... 60

Applicable.....	60
In Review.....	60
Not Applicable.....	63
Insignificant.....	63
Void.....	64

















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

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-wh3p-fphp-9h2m</a>	Arbitrary File Creation in AbstractUnArchiver	2023-07-25	2023-07-25

**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 <b>1.36 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>13.25 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>in review</b> .

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

Target	Hyperlink
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-28115">https://nvd.nist.gov/vuln/detail/CVE-2023-28115</a>

Component	Artifact Id	Version
snappy	snappy-0.4.jar	0.4

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

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-gq6w-q6wh-jggc</a>	PHAR deserialization allowing remote code execution	2023-03-17	2023-03-17

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

<b>Default</b>	No elevated priority.
----------------	-----------------------

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



### 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 <b>1.24 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>13.98 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>in review</b> .

# 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	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-36374">https://nvd.nist.gov/vuln/detail/CVE-2021-36374</a>

## 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

<b>ID</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-5v34-g2px-j4fw</a>	Improper Handling of Length Parameter Inconsistency in Apache Ant	2021-08-02	2021-08-02



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

Id	Summary	Create Date	Update Date
<a href="#">GHSA-q5r4-cfpx-h6fh</a>	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 <b>0.11 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>54.76 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>insignificant</b> .

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	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-36090">https://nvd.nist.gov/vuln/detail/CVE-2021-36090</a>



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

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

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-mc84-pj99-q6hh</a>	Improper Handling of Length Parameter Inconsistency in Compress	2021-08-02	2021-08-02

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

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</a>
Keywords	No keyword sets matched.
EPSS	This vulnerability has a <b>1.37 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>13.20 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>in review</b> .











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

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

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-gwrp-pvrq-jmwv</a>	Path Traversal and Improper Input Validation in Apache Commons IO	2021-04-26	2021-04-26

**Insignificant**   **Default**   **Medium**

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

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N</a>
Keywords	No keyword sets matched.
EPSS	This vulnerability has a <b>0.19 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>42.37 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>insignificant</b> .













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

# 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	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-10683">https://nvd.nist.gov/vuln/detail/CVE-2020-10683</a>

### 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

<b>ID</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-hwj3-m3p6-hj38</a>	dom4j allows External Entities by default which might enable XXE attacks	2020-06-05	2020-06-05

## Assessment

## Summary

## Critical

## CVSS Vector Severity Charts

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 <b>0.66 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>19.90 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>in review</b> .

# 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	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-15756">https://nvd.nist.gov/vuln/detail/CVE-2018-15756</a>

### 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	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



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

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-h436-432x-8fvx</a>	Apache Commons Compress vulnerable to denial of service due to infinite loop	2019-03-14	2019-03-14

☐ Insignificant
 ☐ Default
 ☒ Medium

<b>Default</b>	No elevated priority.
----------------	-----------------------

Criteria	Explanation
CVSS Overall	CVSS:3.1 NVD-CNA-NVD provides the vector: <a href="#">CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</a>
Keywords	No keyword sets matched.
EPSS	This vulnerability has a <b>0.13 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>50.67 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>insignificant</b> .

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.



Target	Hyperlink
CVE	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-1275">https://nvd.nist.gov/vuln/detail/CVE-2018-1275</a>

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

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

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-3rmv-2pg5-xvqj</a>	Improperly Implemented Security Check for Standard in org.springframework:spring-core	2018-10-17	2018-10-17

## Critical

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









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
<a href="#">GHSA-rcpf-vj53-7h2m</a>	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 <b>0.17 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>44.97 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>insignificant</b> .

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	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-1199">https://nvd.nist.gov/vuln/detail/CVE-2018-1199</a>

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

Id	Summary	Create Date	Update Date
<a href="#">GHSA-v596-fwhq-8x48</a>	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 <b>0.18 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>43.86 %</b> of all 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 <b>insignificant</b> .

# 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	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-11771">https://nvd.nist.gov/vuln/detail/CVE-2018-11771</a>

## 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

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-hrmr-f5m6-m9pq</a>	Moderate severity vulnerability that affects org.apache.commons:commons-compress	2018-10-19	2018-10-19

## Assessment

## Summary

## 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:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Keywords	No keyword sets matched.
EPSS	This vulnerability has a <b>0.15 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>48.22 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>insignificant</b> .

# 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 `AbstractJsonResponseBodyAdvice` 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	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-11040">https://nvd.nist.gov/vuln/detail/CVE-2018-11040</a>

## 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

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-f26x-pr96-vw86</a>	Moderate severity vulnerability that affects org.springframework:spring-core	2018-10-16	2018-10-16





## CWE-91

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

## Alerts

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-6pcc-3rfx-4gpm</a>	Dom4j contains a XML Injection vulnerability	2018-10-16	2018-10-16

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

# CVE-2015-7501

### 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.





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 <b>0.88 %</b> chance of being exploited in the next 30 days according to <a href="#">FIRST</a> . It ranks in the top <b>16.88 %</b> of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is <b>in review</b> .

# 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	<a href="https://nvd.nist.gov/vuln/detail/CVE-2015-4035">https://nvd.nist.gov/vuln/detail/CVE-2015-4035</a>

## 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

## Alerts

<b>Id</b>	<b>Summary</b>	<b>Create Date</b>	<b>Update Date</b>
<a href="#">GHSA-mf33-8p24-6h53</a>	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

















## Artifacts

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

## Vulnerabilities

Name	Score	Score <sub>ctx</sub>	Severity	Severity <sub>ctx</sub>	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 12: Maven Core Vulnerabilities

## Artifacts

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

## Vulnerabilities

Name	Score	Score <sub>ctx</sub>	Severity	Severity <sub>ctx</sub>	Priority	Status
<a href="#">CVE-2021-26291</a>	9.1		Critical		Default	In Review
<a href="#">GHSA-2f88-5hg8-9x2x</a>						
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 13: Maven Model Builder Vulnerabilities

## Artifacts

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

## Vulnerabilities

Name	Score	Score <sub>ctx</sub>	Severity	Severity <sub>ctx</sub>	Priority	Status
CVE-2021-26291	9.1		Critical		Default	In Review
	GHSA-2f88-5hg8-9x2x					









Name	Score	Score <sub>ctx</sub>	Severity	Severity <sub>ctx</sub>	Priority	Status
	GHSA-3rmv-2pg5-xvqj					
	GHSA org.springframework:spring-core (Maven) [0, 4.3.16)					
CVE-2018-1272	7.5		High		Default	In Review
	GHSA-4487-x383-qpph					
	GHSA org.springframework:spring-core (Maven) [0, 4.3.15)					
CVE-2018-1271	5.9		Medium		Default	Insignificant
	GHSA-g8hw-794c-4j9g					
	GHSA org.springframework:spring-core (Maven) [0, 4.3.15)					
CVE-2018-1270	9.8		Critical		Escalate	In Review
	GHSA-p5hg-3xm3-gcjq					
	GHSA org.springframework:spring-core (Maven) [0, 4.3.16)					
CVE-2018-1257	6.5		Medium		Default	Insignificant
	GHSA-rcpf-vj53-7h2m					
	GHSA org.springframework:spring-core (Maven) [0, 4.3.17)					
CVE-2018-1199	5.3		Medium		Default	Insignificant
	GHSA-v596-fwhq-8x48					
	GHSA org.springframework:spring-core (Maven) [4.3.0, 4.3.14)					
CVE-2018-11040	7.5		High		Default	In Review
	GHSA-f26x-pr96-vw86					
	GHSA org.springframework:spring-core (Maven) [4.3.0.RELEASE, 4.3.18.RELEASE)					

Table 21: Spring Core Vulnerabilities

## XZ for Java

### Artifacts

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

### Vulnerabilities

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

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

## 5 ae-dita Vulnerability Notice

## 6 ae-dita Vulnerability List

**Applicable**

## In Review

Name	Score	Score <sub>ctx</sub>	Severity	Severity <sub>ctx</sub>	Priority	Status
CVE-2023-41330	9.8		Critical		Default	In Review
	GHSA-92rv-4j2h-8mjj					
	cpe:/a:knplabs:snappy [ , 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-q6wh-jggc					
	cpe:/a:knplabs:snappy [ , 1.4.2)					
CVE-2020-10683	9.8		Critical		Default	In Review
	GHSA-hwj3-m3p6-hj38					
	cpe:/a:dom4j_project:dom4j [ , 2.0.3), GHSA org.dom4j:dom4j (Maven) [0, 2.0.3)					
CVE-2018-1275	9.8		Critical		Default	In Review

Name	Score	Score <sub>ctx</sub>	Severity	Severity <sub>ctx</sub>	Priority	Status
CVE-2018-1270	GHSA-3rmv-2pg5-xvqj					
	GHSA org.springframework:spring-core (Maven) [0, 4.3.16)					
	9.8		Critical		Escalate	In Review
CVE-2015-7501	GHSA-p5hg-3xm3-gcjq					
	GHSA org.springframework:spring-core (Maven) [0, 4.3.16)					
	9.8		Critical		Default	In Review
CVE-2021-26291	GHSA-fjq5-5j5f-mvxh					
	GHSA commons-collections:commons-collections (Maven) [0, 3.2.2)					
	9.1		Critical		Default	In Review
CVE-2022-1271	GHSA-2f88-5hg8-9x2x					
	cpe:/a:apache:maven [, 3.8.1), GHSA org.apache.maven:maven-compat (Maven) [0, 3.8.1), GHSA org.apache.maven:maven-core (Maven) [0, 3.8.1)					
	8.8		High		Default	In Review
CVE-2020-13936	GHSA-jrpw-543v-8r62					
	cpe:/a:tukaani:xz [, 5.2.5)					
	8.8		High		Default	In Review
CVE-2024-47554	GHSA-59j4-wjwp-mw9m					
	GHSA org.apache.velocity:velocity (Maven) [0, 1.7]					
	8.7		High		Default	In Review
CVE-2021-34083	GHSA-78wr-2p64-hpwj					
	GHSA commons-io:commons-io (Maven) [2.0, 2.14.0)					
	8.1		High		Default	In Review
CVE-2015-4035	GHSA-7xhv-mpjw-422f					
	cpe:/a:google-it_project:google-it::~~~node.js~~ [, 1.6.2]					
	7.8		High		Default	In Review
CVE-2021-36090	GHSA-mf33-8p24-6h53					
	cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]					
	7.5		High		Default	In Review
CVE-2021-35517	GHSA-mc84-pj99-q6hh					
	cpe:/a:apache:commons_compress [1.0, 1.21), GHSA org.apache.commons:commons-compress (Maven) [0, 1.21)					
	7.5		High		Default	In Review

Name	Score	Score <sub>ctx</sub>	Severity	Severity <sub>ctx</sub>	Priority	Status
CVE-2021-35516	GHSA-xqfj-vm6h-2x34					
	cpe:/a:apache:commons_compress [1.1, 1.20], GHSA org.apache.commons:commons-compress (Maven) [0, 1.21)					
CVE-2021-35515	7.5		High		Default	In Review
	GHSA-crv7-7245-f45f					
CVE-2018-15756	cpe:/a:apache:commons_compress [1.6, 1.20], GHSA org.apache.commons:commons-compress (Maven) [0, 1.21)					
	7.5		High		Default	In Review
CVE-2018-1272	GHSA-7hfm-57qf-j43q					
	cpe:/a:apache:commons_compress [1.6, 1.20], GHSA org.apache.commons:commons-compress (Maven) [0, 1.21)					
CVE-2018-11040	7.5		High		Default	In Review
	GHSA-ffvq-7w96-97p7					
CVE-2018-1000632	GHSA org.springframework:spring-core (Maven) [4.2.0.RELEASE, 4.3.20.RELEASE)					
	7.5		High		Default	In Review
CVE-2015-6420	GHSA-4487-x383-qpph					
	GHSA org.springframework:spring-core (Maven) [0, 4.3.15)					
CVE-2012-5817	7.5		High		Default	In Review
	GHSA-f26x-pr96-vw86					
CVE-2023-45960	GHSA org.springframework:spring-core (Maven) [4.3.0.RELEASE, 4.3.18.RELEASE)					
	7.5		High		Default	In Review
CVE-2012-5817	GHSA-6pcc-3rfx-4gpm					
	GHSA org.dom4j:dom4j (Maven) [0, 2.0.3)					
CVE-2012-5817	7.5		High		Default	In Review
	GHSA-6hgm-866r-3cjd					
CVE-2012-5817	cpe:/a:apache:commons_collections [, 3.2.1], GHSA commons-collections:commons-collections (Maven) [0, 3.2.2)					
	7.4		High		Default	In Review
CVE-2012-5817	GHSA-5jc8-8xhv-g8qm					
	cpe:/a:codehaus:xfire [, 1.2.6]					
CVE-2012-5817					Default	In Review
	GHSA-fgq9-fc3q-vqmw					



Name	Score	Score <sub>ctx</sub>	Severity	Severity <sub>ctx</sub>	Priority	Status
	GHSA-h436-432x-8fvx					
	cpe:/a:apache:commons_compress [1.11, 1.15], GHSA org.apache.commons:commons-compress (Maven) [1.11, 1.16)					
CVE-2018-11771	5.5		Medium		Default	Insignificant
	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)					
CVE-2018-1002200	5.5		Medium		Default	Insignificant
	GHSA-hcxq-x77q-3469					
	cpe:/a:codehaus-plexus:plexus-archiver [, 3.6.0), GHSA org.codehaus.plexus:plexus-archiver (Maven) [0, 3.6.0)					
CVE-2024-36124	5.3		Medium		Default	Insignificant
	GHSA-8wh2-6qhj-h7j9					
	GHSA org.iq80.snappy:snappy (Maven) [0, 0.5)					
CVE-2018-1199	5.3		Medium		Default	Insignificant
	GHSA-v596-fwhq-8x48					
	GHSA org.springframework:spring-core (Maven) [4.3.0, 4.3.14)					
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 24: Insignificant Category (ae-dita)

## Void

No vulnerabilities are considered `void` within the given configuration.