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

${document.name}

Doc. Identifier: ${document.id}

Doc. Version: ${document.version}

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

Contents

1 ae-core 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-core Affected Assets

No affected assets have been identified.

3 ae-core Vulnerability Details

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

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

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

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2023-45960

Description

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 Reason: This record was withdrawn by its CNA.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

References

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

Affected Components

Component	Artifact Id	Version
	`dom4j-1.6.1.jar`	`1.6.1`

Initial Severity

The vulnerability does not provide any CVSS severity information.

Advisories

Alerts

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GHSA-fgq9-fc3q-vqmw	Withdrawn Advisory: dom4j XML Entity Expansion vulnerability	2023-10-25	2023-10-25

Assessment

Summary

In Review Default

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2023-41330

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

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

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.

Criteria	Explanation
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-3.3.jar`	`3.3`

Weakness

CWE-22

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

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 **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

Description

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

References

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

Affected Components

Component	Artifact Id	Version
snappy	`snappy-0.4.jar`	`0.4`

Weakness

CWE-502

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

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-2022-4245

Description

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

References

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

Affected Components

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

Weakness

CWE-91, CWE-611

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2022-4244

Description

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

References

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

Affected Components

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

Weakness

CWE-22

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2022-29599

Description

In Apache Maven maven-shared-utils prior to version 3.3.3, the Commandline class can emit double-quoted strings without proper escaping, allowing shell injection attacks.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-29599

Affected Components

Component	Artifact Id	Version
Apache Maven Shared Utils	`maven-shared-utils-3.1.0.jar`	`3.1.0`

Weakness

CWE-116

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-rhgr-952r-6p8q	Command injection in Apache Maven maven-shared-utils	2022-05-24	2022-05-24

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 **2.26 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **10.03 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2022-1271

Description

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

References

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

Affected Components

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

Weakness

CWE-179, CWE-20

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **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-2021-4277

Description

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

References

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

Affected Components

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

Weakness

CWE-341, CWE-330

Initial Severity

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

Advisories

Alerts

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

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 **0.06 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **72.31 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **insignificant**.

CVE-2021-3765

Description

validator.js is vulnerable to Inefficient Regular Expression Complexity

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-3765

Affected Components

Component	Artifact Id	Version
Validator	`commons-validator-1.3.1.jar`	`1.3.1`

Weakness
CWE-1333

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
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-qgmg-gppg-76g5	Inefficient Regular Expression Complexity in validator.js	2021-11-03	2021-11-03

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS: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 **0.12 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **53.01 %** of all scored vulnerabilities.
KEV	This vulnerability 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-2021-35939

Description

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

References

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

Affected Components

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

Weakness

CWE-59

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default **Medium**

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

Criteria	Explanation
Assessment	The vulnerability status is **insignificant**.

CVE-2021-35938

Description

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

References

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

Affected Components

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

Weakness

CWE-59

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2021-35937

Description

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

References

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

Affected Components

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

Weakness

CWE-59, CWE-367

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default **Medium**

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2021-3521

Description

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

References

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

Affected Components

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

Weakness

CWE-347

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant **Default** **Medium**

CVSS Vector Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2021-3421

Description

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

References

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

Affected Components

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

Weakness

CWE-347

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

Criteria	Explanation
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 Core	`maven-core-3.0.5.jar`	`3.0.5`
Maven Plugin Tools Java 5 Annotations	`maven-plugin-annotations-3.5.jar`	`3.5`
Maven Model Builder	`maven-model-builder-3.0.5.jar`	`3.0.5`
Maven Incremental Build support utilities	`maven-shared-incremental-1.1.jar`	`1.1`
Maven Model	`maven-model-3.0.5.jar`	`3.0.5`
Maven Aether Provider	`maven-aether-provider-3.0.5.jar`	`3.0.5`
Apache Maven Archiver	`maven-archiver-3.1.1.jar`	`3.1.1`
Maven Compat	`maven-compat-3.0.5.jar`	`3.0.5`
Maven Repository Metadata Model	`maven-repository-metadata-3.0.5.jar`	`3.0.5`
Apache Maven Compiler Plugin	`maven-compiler-plugin-3.6.2.jar`	`3.6.2`
Apache Maven Wagon :: API	`wagon-provider-api-2.4.jar`	`2.4`
Maven Plugin API	`maven-plugin-api-3.0.5.jar`	`3.0.5`
Maven Settings Builder	`maven-settings-builder-3.0.5.jar`	`3.0.5`
Maven Settings	`maven-settings-3.0.5.jar`	`3.0.5`
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

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

Advisories

Alerts

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

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:N
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **0.20 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **41.61 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2021-20266

Description

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

References

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

Affected Components

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

Weakness
CWE-125

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant **Default** **Medium**

CVSS Vector Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2020-13959

Description

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

References

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

Affected Components

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

Weakness

CWE-79

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant **Default** **Medium**

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2020-13936

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`velocity-1.7.jar`	`1.7`

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

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

Id	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

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

CVE-2020-10519

Description

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

References

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

Affected Components

Component	Artifact Id	Version
Package URL	`packageurl-java-1.5.0.jar`	`1.5.0`
curvesapi	`curvesapi-1.08.jar`	`1.08`

Weakness
CWE-77

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	8.8	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`	High
CVSS:2.0	NVD-CNA-NVD	6.5	`AV:N/AC:L/Au:S/C:P/I:P/A:P`	Medium

Advisories

Alerts

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

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **0.71 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **18.99 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2020-10518

Description

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

References

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

Affected Components

Component	Artifact Id	Version
Package URL	`packageurl-java-1.5.0.jar`	`1.5.0`
curvesapi	`curvesapi-1.08.jar`	`1.08`

Weakness

CWE-77

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	8.8	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`	High
CVSS:2.0	NVD-CNA-NVD	6.5	`AV:N/AC:L/Au:S/C:P/I:P/A:P`	Medium

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2020-10517

Description

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

References

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

Affected Components

Component	Artifact Id	Version
Package URL	`packageurl-java-1.5.0.jar`	`1.5.0`
curvesapi	`curvesapi-1.08.jar`	`1.08`

Weakness

CWE-285

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	4.3	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N`	Medium
CVSS:2.0	NVD-CNA-NVD	4.0	`AV:N/AC:L/Au:S/C:P/I:N/A:N`	Medium

Advisories

Alerts

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

Assessment

Summary

Insignificant **Default** **Medium**

CVSS Vector Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2019-10202

Description

A series of deserialization vulnerabilities have been discovered in Codehaus 1.9.x implemented in EAP 7. This CVE fixes CVE-2017-17485, CVE-2017-7525, CVE-2017-15095, CVE-2018-5968, CVE-2018-7489, CVE-2018-1000873, CVE-2019-12086 reported for FasterXML jackson-databind by implementing a whitelist approach that will mitigate these vulnerabilities and future ones alike.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-10202

Affected Components

Component	Artifact Id	Version
Data Mapper for Jackson	`jackson-mapper-asl-1.9.13.jar`	`1.9.13`

Weakness

CWE-502

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	GitHub, Inc.	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-c27h-mcmw-48hv	Deserialization of Untrusted Data in org.codehaus.jackson:jackson-mapper-asl	2022-05-24	2022-05-24

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 GitHub, Inc.* 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 **1.94 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **10.86 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2019-10172

Description

A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-asl libraries but in different classes.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2019-10172

Affected Components

Component	Artifact Id	Version
Data Mapper for Jackson	`jackson-mapper-asl-1.9.13.jar`	`1.9.13`

Weakness

CWE-611

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: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-r6j9-8759-g62w	Improper Restriction of XML External Entity Reference in jackson-mapper-asl	2020-02-04	2020-02-04

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 GitHub, Inc.* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N`

Criteria	Explanation
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 **40.84 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2018-6969

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`tools-1.8.0.jar`	`1.8.0`

Weakness

CWE-125

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale
The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2018-1002200

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-3.3.jar`	`3.3`

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

In Review Default High

CVSS Vector Severity Charts

Rationale
The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2017-9530

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`tools-1.8.0.jar`	`1.8.0`

Weakness

CWE-119

Initial Severity

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-cx97-5qm7-6wq7	IrfanView version 4.44 (32bit) might allow attackers to cause a denial of service or execute arbitrary code via a crafted file, related to "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at ntdll_77df0000! LdrpResCompareResourceNames+0x0000000000000150."	2022-05-17	2022-05-17

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

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

CVE-2017-7501

Description

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

References

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

Affected Components

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

Weakness

CWE-59

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.8	`CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`	High
CVSS:2.0	NVD-CNA-NVD	4.6	`AV:L/AC:L/Au:N/C:P/I:P/A:P`	Medium

Advisories

Alerts

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

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale
The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2017-1000487

Description

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

References

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

Affected Components

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

Weakness
CWE-78

Initial Severity

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

Advisories

Alerts

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

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 **0.39 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **25.82 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2016-7080

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`tools-1.8.0.jar`	`1.8.0`

Weakness

CWE-476

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.8	`CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`	High
CVSS:2.0	NVD-CNA-NVD	4.6	`AV:L/AC:L/Au:N/C:P/I:P/A:P`	Medium

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2016-7079

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`tools-1.8.0.jar`	`1.8.0`

Weakness
CWE-476

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	High
CVSS:2.0	NVD-CNA-NVD	4.6	AV:L/AC:L/Au:N/C:P/I:P/A:P	Medium

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale
The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2016-5328

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`tools-1.8.0.jar`	`1.8.0`

Weakness
CWE-200

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

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

Criteria	Explanation
Assessment	The vulnerability status is **insignificant**.

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.

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

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 **2.47 %** 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

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS: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-2015-5191

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`tools-1.8.0.jar`	`1.8.0`

Weakness

CWE-362

Initial Severity

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

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:2.0	NVD-CNA-NVD	3.7	AV:L/AC:H/Au:N/C:P/I:P/A:P	Low

Advisories

Alerts

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

Assessment

Summary

Insignificant Default **Medium**

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2015-4035

Description

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

References

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

Affected Components

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

Weakness

CWE-20

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	7.8	`CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`	High
CVSS:2.0	NVD-CNA-NVD	4.6	`AV:L/AC:L/Au:N/C:P/I:P/A:P`	Medium

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV: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-2014-8118

Description

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

References

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

Affected Components

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

Weakness

CWE-189

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default Critical

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

Criteria	Explanation
EPSS	This vulnerability has a **36.79 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **2.71 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2014-4200

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`tools-1.8.0.jar`	`1.8.0`

Weakness

CWE-264

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant **Default** **Medium**

CVSS Vector Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2014-4199

Description

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

References

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

Affected Components

Component	Artifact Id	Version
	`tools-1.8.0.jar`	`1.8.0`

Weakness
CWE-59

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2013-6435

Description

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

References

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

Affected Components

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

Weakness

CWE-74

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2012-2055

Description

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

References

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

Affected Components

Component	Artifact Id	Version
Package URL	`packageurl-java-1.5.0.jar`	`1.5.0`

Weakness
CWE-913

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale
The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2012-0815

Description

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

References

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

Affected Components

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

Weakness

CWE-189

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

Criteria	Explanation
Assessment	The vulnerability status is **insignificant**.

CVE-2012-0061

Description

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

References

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

Affected Components

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

Weakness

CWE-20

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2012-0060

Description

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

References

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

Affected Components

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

Weakness

CWE-20

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant Default **Medium**

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2011-3378

Description

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

References

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

Affected Components

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

Weakness

CWE-94

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2010-2199

Description

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

References

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

Affected Components

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

Weakness

CWE-264

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2010-2198

Description

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

References

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

Affected Components

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

Weakness

CWE-264

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2010-2197

Description

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

References

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

Affected Components

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

Weakness

CWE-264

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

Insignificant **Default** **Medium**

CVSS Vector Severity Charts

Rationale
Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2010-2059

Description

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

References

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

Affected Components

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

Weakness
CWE-264

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

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

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

CVE-2005-4889

Description

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

References

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

Affected Components

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

Weakness
CWE-264

Initial Severity

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

Advisories

Alerts

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

Assessment

Summary

In Review Default High

CVSS Vector Severity Charts

Rationale
The vulnerability has automatically been marked as in review.

Priority

Default No elevated priority.

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

4 ae-core Affected Components

Package URL

Artifacts

Component	Artifact Id	Version
Package URL	`packageurl-java-1.5.0.jar`	`1.5.0`

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
`CVE-2020-10519`	8.8		High		Default	In Review
	GHSA-gcp3-gfr7-rcqp					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.20.24)					
`CVE-2020-10518`	8.8		High		Default	In Review
	GHSA-m5vm-44r4-56mf					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)					
`CVE-2020-10517`	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7-6jvw					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)					
`CVE-2012-2055`	7.5		High		Default	In Review
	GHSA-8qp2-79w8-8586					
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)					

Table 1: Package URL Vulnerabilities

curvesapi

Artifacts

Component	Artifact Id	Version
curvesapi	`curvesapi-1.08.jar`	`1.08`

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
`CVE-2020-10519`	8.8		High		Default	In Review
	GHSA-gcp3-gfr7-rcqp					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.20.24)					

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
CVE-2020-10518	8.8		High		Default	In Review
	GHSA-m5vm-44r4-56mf					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)					
CVE-2020-10517	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7-6jvw					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)					

Table 2: curvesapi 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 3: Commons Collections Vulnerabilities

Validator

Artifacts

Component	Artifact Id	Version
Validator	`commons-validator-1.3.1.jar`	`1.3.1`

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
CVE-2021-3765	5.3		Medium		Default	Insignificant
	GHSA-qgmg-gppg-76g5					

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
	cpe:/a:validator_project:validator:::~~~node.js~~ [, 13.7.0)					

Table 4: Validator 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 5: Maven Plugin Tools Java 5 Annotations Vulnerabilities

Apache Maven Compiler Plugin

Artifacts

Component	Artifact Id	Version
Apache Maven Compiler Plugin	`maven-compiler-plugin-3.6.2.jar`	`3.6.2`

Vulnerabilities

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

Table 6: Apache Maven Compiler Plugin Vulnerabilities

Maven Incremental Build support utilities

Artifacts

Component	Artifact Id	Version
Maven Incremental Build support utilities	`maven-shared-incremental-1.1.jar`	`1.1`

Vulnerabilities

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

Table 7: Maven Incremental Build support utilities Vulnerabilities

Apache Maven Shared Utils

Artifacts

Component	Artifact Id	Version
Apache Maven Shared Utils	maven-shared-utils-3.1.0.jar	3.1.0

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
CVE-2022-29599	9.8		Critical		Default	In Review
	GHSA-rhgr-952r-6p8q					
	cpe:/a:apache:maven_shared_utils [, 3.3.3), GHSA org.apache.maven.shared:maven-shared-utils (Maven) [0, 3.3.3)					

Table 8: Apache Maven Shared Utils 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 9: 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 10: 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 11: 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					

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 12: Maven Compat Vulnerabilities

Maven Core

Artifacts

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

Vulnerabilities

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

Table 13: 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:maven-core (Maven) [0, 3.8.1)					

Table 14: Maven Model Builder Vulnerabilities

Maven Model

Artifacts

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

Vulnerabilities

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

Table 15: 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)					

Table 16: Maven Plugin API Vulnerabilities

Maven Repository Metadata Model

Artifacts

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

Vulnerabilities

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

Table 17: Maven Repository Metadata Model Vulnerabilities

Maven Settings Builder

Artifacts

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

Vulnerabilities

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

Table 18: Maven Settings Builder Vulnerabilities

Maven Settings

Artifacts

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

Vulnerabilities

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

Table 19: Maven Settings Vulnerabilities

Apache Maven Archiver

Artifacts

Component	Artifact Id	Version
Apache Maven Archiver	`maven-archiver-3.1.1.jar`	`3.1.1`

Vulnerabilities

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

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 20: Apache Maven Archiver Vulnerabilities

VelocityTools

Artifacts

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

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
`CVE-2020-13959`	6.1		Medium		Default	Insignificant
	GHSA-fh63-4r66-jc7v					
	cpe:/a:apache:velocity_tools [, 3.1), GHSA org.apache.velocity:velocity-tools (Maven) [0, 2.0]					

Table 21: VelocityTools Vulnerabilities

Data Mapper for Jackson

Artifacts

Component	Artifact Id	Version
Data Mapper for Jackson	`jackson-mapper-asl-1.9.13.jar`	`1.9.13`

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
`CVE-2019-10202`	9.8		Critical		Default	In Review
	GHSA-c27h-mcmw-48hv					
	GHSA org.codehaus.jackson:jackson-mapper-asl (Maven) [0, 1.9.13]					
`CVE-2019-10172`	7.5		High		Default	In Review
	GHSA-r6j9-8759-g62w					
	cpe:/a:fasterxml:jackson-mapper-asl [1.9.0, 1.9.13], GHSA org.codehaus.jackson:jackson-mapper-asl (Maven) [0, 1.9.13]					

Table 22: Data Mapper for Jackson Vulnerabilities

Plexus Common Utilities

Artifacts

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

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
`CVE-2022-4245`	4.3		Medium		Default	Insignificant
	GHSA-jcwr-x25h-x5fh					
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.24), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.24)					
`CVE-2022-4244`	7.5		High		Default	In Review
	GHSA-g6ph-x5wf-g337					
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.24), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.24)					
`CVE-2017-1000487`	9.8		Critical		Default	In Review
	GHSA-8vhq-qq4p-grq3					
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.16), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.16)					

Table 23: Plexus Common Utilities Vulnerabilities

Plexus Archiver Component

Artifacts

Component	Artifact Id	Version
Plexus Archiver Component	`plexus-archiver-3.3.jar`	`3.3`

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
`CVE-2023-37460`	9.8		Critical		Default	In Review
	GHSA-wh3p-fphp-9h2m					
	cpe:/a:codehaus-plexus:plexus-archiver [, 4.8.0), GHSA org.codehaus.plexus:plexus-archiver (Maven) [0, 4.8.0)					
`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)					

Table 24: 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.snappy:snappy (Maven) [0, 0.5)					
`CVE-2023-41330`	9.8		Critical		Default	In Review
	GHSA-92rv-4j2h-8mjj					
	cpe:/a:knplabs:snappy [, 1.4.3)					
`CVE-2023-28115`	9.8		Critical		Default	In Review
	GHSA-gq6w-q6wh-jggc					
	cpe:/a:knplabs:snappy [, 1.4.2)					

Table 25: snappy Vulnerabilities

XZ for Java

Artifacts

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

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
`CVE-2022-1271`	8.8		High		Default	In Review
	GHSA-jrpw-543v-8r62					
	cpe:/a:tukaani:xz [, 5.2.5)					
`CVE-2015-4035`	7.8		High		Default	In Review
	GHSA-mf33-8p24-6h53					
	cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]					

Table 26: XZ for Java Vulnerabilities

5 ae-core Vulnerability Notice

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

6 ae-core 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$_{\text{ctx}}$	Severity	Severity$_{\text{ctx}}$	Priority	Status
CVE-2014-8118	10.0		Critical		Default	In Review
	GHSA-wj3v-j872-6xqx					
	cpe:/a:rpm:rpm [, 4.12.0]					
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-2022-29599	9.8		Critical		Default	In Review
	GHSA-rhgr-952r-6p8q					
	cpe:/a:apache:maven_shared_utils [, 3.3.3), GHSA org.apache.maven.shared:maven-shared-utils (Maven) [0, 3.3.3)					
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)					

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
CVE-2019-10202	9.8		Critical		Default	In Review
	GHSA-c27h-mcmw-48hv					
	GHSA org.codehaus.jackson:jackson-mapper-asl (Maven) [0, 1.9.13]					
CVE-2017-1000487	9.8		Critical		Default	In Review
	GHSA-8vhq-qq4p-grq3					
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.16), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.16)					
CVE-2015-7501	9.8		Critical		Default	In Review
	GHSA-fjq5-5j5f-mvxh					
	GHSA commons-collections:commons-collections (Maven) [0, 3.2.2)					
CVE-2011-3378	9.3		Critical		Default	In Review
	GHSA-34ff-v8wx-w9f5					
	cpe:/a:rpm:rpm [, 4.9.1.1]					
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)					
CVE-2022-1271	8.8		High		Default	In Review
	GHSA-jrpw-543v-8r62					
	cpe:/a:tukaani:xz [, 5.2.5)					
CVE-2020-13936	8.8		High		Default	In Review
	GHSA-59j4-wjwp-mw9m					
	GHSA org.apache.velocity:velocity (Maven) [0, 1.7]					
CVE-2020-10519	8.8		High		Default	In Review
	GHSA-gcp3-gfr7-rcqp					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.20.24)					
CVE-2020-10518	8.8		High		Default	In Review
	GHSA-m5vm-44r4-56mf					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)					
CVE-2017-9530	7.8		High		Default	In Review
	GHSA-cx97-5qm7-6wq7					
	cpe:/a:irfanview:tools [, 4.50]					
CVE-2017-7501	7.8		High		Default	In Review

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
	GHSA-3xgr-x5gv-64gh					
	cpe:/a:rpm:rpm [, 4.13.0.3)					
CVE-2016-7080	7.8		High		Default	In Review
	GHSA-cp2g-849g-w9jr					
	cpe:/a:vmware:tools [, 10.0.8]					
CVE-2016-7079	7.8		High		Default	In Review
	GHSA-wxpj-3x4g-grwp					
	cpe:/a:vmware:tools [, 10.0.8]					
CVE-2015-4035	7.8		High		Default	In Review
	GHSA-mf33-8p24-6h53					
	cpe:/a:tukaani:xz::beta * (beta)[, 4.999.9]					
CVE-2013-6435	7.6		High		Default	In Review
	GHSA-qww5-w98g-66q7					
	cpe:/a:rpm:rpm [, 4.11.1]					
CVE-2022-4244	7.5		High		Default	In Review
	GHSA-g6ph-x5wf-g337					
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.24), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.24)					
CVE-2019-10172	7.5		High		Default	In Review
	GHSA-r6j9-8759-g62w					
	cpe:/a:fasterxml:jackson-mapper-asl [1.9.0, 1.9.13], GHSA org.codehaus.jackson:jackson-mapper-asl (Maven) [0, 1.9.13]					
CVE-2018-1000632	7.5		High		Default	In Review
	GHSA-6pcc-3rfx-4gpm					
	GHSA org.dom4j:dom4j (Maven) [0, 2.0.3)					
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)					
CVE-2012-2055	7.5		High		Default	In Review
	GHSA-8qp2-79w8-8586					
	cpe:/a:github:github:::~~enterprise~~~ [, 20120304)					
CVE-2010-2199	7.2		High		Default	In Review

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
	GHSA-7v29-vf8p-2rvp					
	cpe:/a:rpm:rpm [, 4.8.0]					
CVE-2010-2198	7.2		High		Default	In Review
	GHSA-fw46-vp2w-pvxq					
	cpe:/a:rpm:rpm [, 4.8.0]					
CVE-2010-2059	7.2		High		Default	In Review
	GHSA-f3f6-q22p-8fh5					
	cpe:/a:rpm:rpm [, 4.4.2.3]					
CVE-2005-4889	7.2		High		Default	In Review
	GHSA-pfqv-vjx4-pmxj					
	cpe:/a:rpm:rpm [, 4.4.2.3]					
CVE-2018-6969	7.0		High		Default	In Review
	GHSA-qc3q-9h28-r994					
	cpe:/a:vmware:tools [, 10.3.0)					
CVE-2023-45960					Default	In Review
	GHSA-fgq9-fc3q-vqmw					
	GHSA org.dom4j:dom4j (Maven) [0, 2.1.4]					

Table 27: In Review Category (ae-core)

Not Applicable

No vulnerabilities are considered `Not Applicable` within the given configuration.

Insignificant

The following vulnerabilities are considered `Insignificant` within the given configuration:

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
CVE-2012-0815	6.8		Medium		Default	Insignificant
	CERT-EU-2012-0126 GHSA-6grx-55mc-2wmq					
	cpe:/a:rpm:rpm [, 4.9.1.2]					
CVE-2012-0061	6.8		Medium		Default	Insignificant
	CERT-EU-2012-0126 GHSA-v3v4-hffr-vr89					

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
	cpe:/a:rpm:rpm [, 4.9.1.2]					
CVE-2012-0060	6.8		Medium		Default	Insignificant
	CERT-EU-2012-0126 GHSA-j6wj-cqmg-hvcm					
	cpe:/a:rpm:rpm [, 4.9.1.2]					
CVE-2021-35939	6.7		Medium		Default	Insignificant
	GHSA-prgv-w33h-5m73					
	cpe:/a:rpm:rpm [, 4.18)					
CVE-2021-35938	6.7		Medium		Default	Insignificant
	GHSA-83gm-5269-qr3v					
	cpe:/a:rpm:rpm [, 4.18.0)					
CVE-2015-5191	6.7		Medium		Default	Insignificant
	GHSA-4vr2-36wr-v82r					
	cpe:/a:vmware:tools [, 10.0.8]					
CVE-2021-35937	6.4		Medium		Default	Insignificant
	GHSA-63x9-9q4w-j636					
	cpe:/a:rpm:rpm [, 4.18.0)					
CVE-2014-4199	6.3		Medium		Default	Insignificant
	GHSA-v55p-68fc-xxcv					
	cpe:/a:vmware:tools					
CVE-2020-13959	6.1		Medium		Default	Insignificant
	GHSA-fh63-4r66-jc7v					
	cpe:/a:apache:velocity_tools [, 3.1), GHSA org.apache.velocity:velocity-tools (Maven) [0, 2.0]					
CVE-2010-2197	5.8		Medium		Default	Insignificant
	GHSA-6gj2-w23f-chf3					
	cpe:/a:rpm:rpm [, 4.8.0]					
CVE-2021-3421	5.5		Medium		Default	Insignificant
	GHSA-f7ww-c7v4-g682					
	cpe:/a:rpm:rpm [, 4.16.1.3)					
CVE-2018-1002200	5.5		Medium		Default	Insignificant
	GHSA-hcxq-x77q-3469					

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
	cpe:/a:codehaus-plexus:plexus-archiver [, 3.6.0), GHSA org.codehaus.plexus:plexus-archiver (Maven) [0, 3.6.0)					
CVE-2016-5328	5.5		Medium		Default	Insignificant
	GHSA-4h47-vq45-ccw2					
	cpe:/a:vmware:tools [, 10.0.8]					
CVE-2024-36124	5.3		Medium		Default	Insignificant
	GHSA-8wh2-6qhj-h7j9					
	GHSA org.iq80.snappy:snappy (Maven) [0, 0.5)					
CVE-2021-4277	5.3		Medium		Default	Insignificant
	GHSA-3cqm-26w8-85g8					
	cpe:/a:utils_project:utils [, 2021-05-14)					
CVE-2021-3765	5.3		Medium		Default	Insignificant
	GHSA-qgmg-gppg-76g5					
	cpe:/a:validator_project:validator:::~~~node.js~~ [, 13.7.0)					
CVE-2021-20266	4.9		Medium		Default	Insignificant
	GHSA-8vf3-43pf-v3cq					
	cpe:/a:rpm:rpm [, 4.16.1.3)					
CVE-2021-3521	4.7		Medium		Default	Insignificant
	GHSA-pr6x-p264-jrpq					
	cpe:/a:rpm:rpm [, 4.17.1)					
CVE-2014-4200	4.7		Medium		Default	Insignificant
	GHSA-959q-xwwj-g697					
	cpe:/a:vmware:tools					
CVE-2022-4245	4.3		Medium		Default	Insignificant
	GHSA-jcwr-x25h-x5fh					
	cpe:/a:codehaus-plexus:plexus-utils [, 3.0.24), GHSA org.codehaus.plexus:plexus-utils (Maven) [0, 3.0.24)					
CVE-2020-10517	4.3		Medium		Default	Insignificant
	GHSA-38rx-7wc7-6jvw					
	cpe:/a:github:github:::~~enterprise~~~ [, 2.19.21)					

Table 28: Insignificant Category (ae-core)

Void

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