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

${document.name}

Doc. Identifier: ${document.id}

Doc. Version: ${document.version}

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

Contents

1 example 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 example Affected Assets

No affected assets have been identified.

3 example Vulnerability Details

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

CVE-2024-38820

Description

The fix for CVE-2022-22968 made disallowedFields patterns in DataBinder case insensitive. However, String.toLowerCase() has some Locale dependent exceptions that could potentially result in fields not protected as expected.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2024-38820

Affected Components

Component	Artifact Id	Version
	`spring-context-5.3.14.jar`	`5.3.14`

Weakness

CWE-178

Initial Severity

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-4gc7-5j7h-4qph	Spring Framework DataBinder Case Sensitive Match Exception	2024-10-18	2024-10-18

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N`
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 **76.57 %** 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 **insignificant**.

CVE-2024-38808

Description

In Spring Framework versions 5.3.0 - 5.3.38 and older unsupported versions, it is possible for a user to provide a specially crafted Spring Expression Language (SpEL) expression that may cause a denial of service (DoS) condition. Specifically, an application is vulnerable when the following is true: * The application evaluates user-supplied SpEL expressions.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2024-38808

Affected Components

Component	Artifact Id	Version
	spring-expression-5.3.14.jar	5.3.14

Weakness

CWE-770

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:4.0	GitHub, Inc.	5.1	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N	Medium
CVSS:3.1	GitHub, Inc.	4.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-9cmq-m9j5-mvww	Spring Framework vulnerable to Denial of Service	2024-08-20	2024-08-20

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

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

CVE-2023-20863

Description

In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-20863

Affected Components

Component	Artifact Id	Version
	`spring-expression-5.3.14.jar`	`5.3.14`

Weakness

CWE-400, CWE-917

Initial Severity

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-wxqc-pxw9-g2p8	Spring Framework vulnerable to denial of service	2023-04-13	2023-04-13

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:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/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 **44.78 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **insignificant**.

CVE-2023-20861

Description

In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2023-20861

Affected Components

Component	Artifact Id	Version
	`spring-expression-5.3.14.jar`	`5.3.14`

Initial Severity

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-564r-hj7v-mcr5	Spring Framework vulnerable to denial of service via specially crafted SpEL expression	2023-03-23	2023-03-23

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:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **0.12 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **52.26 %** of all scored vulnerabilities.
KEV	This vulnerability 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-2022-22970

Description

In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-22970

Affected Components

Component	Artifact Id	Version
	`spring-beans-5.3.14.jar`	`5.3.14`

Weakness

CWE-770

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	5.3	`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H`	Medium
CVSS:2.0	NVD-CNA-NVD	3.5	`AV:N/AC:M/Au:S/C:N/I:N/A:P`	Low

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-hh26-6xwr-ggv7	Denial of service in Spring Framework	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:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **0.45 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **24.21 %** 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-2022-22968

Description

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-22968

Affected Components

Component	Artifact Id	Version
	`spring-context-5.3.14.jar`	`5.3.14`

Weakness

CWE-178

Initial Severity

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

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-g5mm-vmx4-3rg7	Improper handling of case sensitivity in Spring Framework	2022-04-15	2022-04-15

Assessment

Summary

Insignificant Default **Medium**

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/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 **67.81 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **insignificant**.

CVE-2022-22965

Description

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-22965

Affected Components

Component	Artifact Id	Version
	`spring-beans-5.3.14.jar`	`5.3.14`

Weakness

CWE-94

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-36p3-wjmg-h94x	Remote Code Execution in Spring Framework	2022-03-31	2022-03-31
CERT-EU-2022-023	UPDATE: Critical RCE Vulnerability in Spring Core	2022-03-31	2022-03-31

Assessment

Summary

In Review Escalate Critical

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (**13.7** from base score **9.8**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **97.50 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **0.01 %** of all scored vulnerabilities.
KEV	This vulnerability, affecting **VMware Spring Framework**, has been **confirmed to have been exploited in the wild**. **Summary:** Spring Framework JDK 9+ Remote Code Execution Vulnerability. Apply updates per vendor instructions. **Notes:** https://nvd.nist.gov/vuln/detail/CVE-2022-22965 **Due Date:** 2022-04-25 **Publish Date:** 2022-04-04
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2022-22950

Description

n Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2022-22950

Affected Components

Component	Artifact Id	Version
	spring-expression-5.3.14.jar	5.3.14

Weakness

CWE-770

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.5	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	Medium
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-558x-2xjg-6232	Allocation of Resources Without Limits or Throttling in Spring Framework	2022-04-03	2022-04-03

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

Criteria	Explanation
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **0.08 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **63.64 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **insignificant**.

CVE-2021-45105

Description

Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-45105

Affected Components

Component	Artifact Id	Version
log4j-api	`log4j-api-2.14.0.jar`	`2.14.0`
log4j-core	`log4j-core-2.14.0.jar`	`2.14.0`

Weakness

CWE-20

Initial Severity

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

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-p6xc-xr62-6r2g	Apache Log4j2 vulnerable to Improper Input Validation and Uncontrolled Recursion	2021-12-18	2021-12-18
CERT-EU-2021-067	UPDATE: Java Logging Package RCE Vulnerability	2021-12-10	2021-12-10

Assessment

Summary

Insignificant **Due** **Medium**

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Due (**7.8** from base score **5.9**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **96.00 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **0.45 %** 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-2021-45046

Description

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-45046

Affected Components

Component	Artifact Id	Version
log4j-api	`log4j-api-2.14.0.jar`	`2.14.0`
log4j-core	`log4j-core-2.14.0.jar`	`2.14.0`

Weakness

CWE-917

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	9.0	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H`	Critical
CVSS:2.0	NVD-CNA-NVD	5.1	`AV:N/AC:H/Au:N/C:P/I:P/A:P`	Medium

Advisories

Alerts

Id	Summary	Create Date	Update Date
CERT-EU-2021-075	VMWare Critical Vulnerability	2021-12-18	2021-12-18
GHSA-7rjr-3q55-vv33	Incomplete fix for Apache Log4j vulnerability	2021-12-14	2021-12-14
CERT-EU-2021-067	UPDATE: Java Logging Package RCE Vulnerability	2021-12-10	2021-12-10
CERT-EU-2021-076	Fortinet Critical Vulnerability	2021-12-18	2021-12-18

Assessment

Summary

In Review Escalate Critical

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (**13.9** from base score **9.0**)

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **97.29 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **0.10 %** of all scored vulnerabilities.
KEV	This vulnerability, affecting **Apache Log4j2**, has been **confirmed to have been exploited in the wild**. Furthermore, it has been **identified in ransomware campaigns**. **Summary:** Apache Log4j2 Deserialization of Untrusted Data Vulnerability. Apply updates per vendor instructions. **Notes:** https://logging.apache.org/log4j/2.x/security.html; https://nvd.nist.gov/vuln/detail/CVE-2021-45046 **Due Date:** 2023-05-22 **Publish Date:** 2023-05-01
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

CVE-2021-44832

Description

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-44832

Affected Components

Component	Artifact Id	Version
log4j-api	`log4j-api-2.14.0.jar`	`2.14.0`
log4j-core	`log4j-core-2.14.0.jar`	`2.14.0`

Weakness

CWE-20

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	6.6	`CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H`	Medium
CVSS:2.0	NVD-CNA-NVD	8.5	`AV:N/AC:M/Au:S/C:C/I:C/A:C`	High

Advisories

Alerts

Id	Summary	Create Date	Update Date
GHSA-8489-44mv-ggj8	Improper Input Validation and Injection in Apache Log4j2	2022-01-04	2022-01-04
CERT-EU-2021-067	UPDATE: Java Logging Package RCE Vulnerability	2021-12-10	2021-12-10

Assessment

Summary

Insignificant Default Medium

CVSS Vector Severity Charts

Rationale

Score is below 7,0

Priority

Default No elevated priority.

Criteria	Explanation
CVSS Overall	*CVSS:3.1 NVD-CNA-NVD* provides the vector: `CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **2.24 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **10.07 %** of all scored vulnerabilities.
KEV	This vulnerability has not been confirmed to have been exploited in the wild.
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **insignificant**.

CVE-2021-44228

Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

References

Target	Hyperlink
CVE	https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Affected Components

Component	Artifact Id	Version
log4j-api	`log4j-api-2.14.0.jar`	`2.14.0`
log4j-core	`log4j-core-2.14.0.jar`	`2.14.0`

Weakness

CWE-20, CWE-917

Initial Severity

Scheme	Source	Overall	CVSS Vector	Severity
CVSS:3.1	NVD-CNA-NVD	10.0	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`	Critical
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
CERT-EU-2021-070	MobileIron Critical Vulnerability	2021-12-16	2021-12-16
CERT-EU-2021-075	VMWare Critical Vulnerability	2021-12-18	2021-12-18
CERT-EU-2021-072	ArcGIS Critical Vulnerability	2021-12-16	2021-12-16

Id	Summary	Create Date	Update Date
CERT-EU-2022-005	Critical Vulnerability in Ivanti Products	2022-01-19	2022-01-19
GHSA-jfh8-c2jp-5v3q	Remote code injection in Log4j	2021-12-10	2021-12-10
CERT-EU-2021-074	CISCO Critical Vulnerability	2021-12-18	2021-12-18
CERT-EU-2021-073	Adobe ColdFusion Critical Vulnerability	2021-12-17	2021-12-17
CERT-EU-2021-067	UPDATE: Java Logging Package RCE Vulnerability	2021-12-10	2021-12-10
CERT-EU-2021-071	UPDATE: Palo Alto Critical Vulnerability	2021-12-16	2021-12-16
CERT-EU-2021-076	Fortinet Critical Vulnerability	2021-12-18	2021-12-18

Assessment

Summary

In Review **Escalate** **Critical**

CVSS Vector Severity Charts

Rationale

The vulnerability has automatically been marked as in review.

Priority

Escalate (**14.9** from base score **10.0**)

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:C/C:H/I:H/A:H`
Keywords	No keyword sets matched.
EPSS	This vulnerability has a **96.89 %** chance of being exploited in the next 30 days according to FIRST. It ranks in the top **0.24 %** of all scored vulnerabilities.
KEV	This vulnerability, affecting **Apache Log4j2**, has been **confirmed to have been exploited in the wild**. Furthermore, it has been **identified in ransomware campaigns**. **Summary:** Apache Log4j2 Remote Code Execution Vulnerability. For all affected software assets for which updates exist, the only acceptable remediation actions are: 1) Apply updates; OR 2) remove affected assets from agency networks. Temporary mitigations using one of the measures provided at https://www.cisa.gov/uscert/ed-22-02-apache-log4j-recommended-mitigation-measures are only acceptable until updates are available. **Notes:** https://nvd.nist.gov/vuln/detail/CVE-2021-44228 **Due Date:** 2021-12-24 **Publish Date:** 2021-12-10
EOL	No end-of-life (EOL) information available.
Assessment	The vulnerability status is **in review**.

4 example Affected Components

log4j-core

Artifacts

Component	Artifact Id	Version
log4j-core	`log4j-core-2.14.0.jar`	`2.14.0`

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
`CVE-2021-45105`	5.9		Medium		Due	Insignificant
	CERT-EU-2021-067 GHSA-p6xc-xr62-6r2g					
	cpe:/a:apache:log4j [2.13.0, 2.16.0], GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.17.0)					
`CVE-2021-45046`	9.0		Critical		Escalate	In Review
	CERT-EU-2021-075, CERT-EU-2021-067, CERT-EU-2021-076 GHSA-7rjr-3q55-vv33					
	cpe:/a:apache:log4j [2.13.0, 2.16.0), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.16.0)					
`CVE-2021-44832`	6.6		Medium		Default	Insignificant
	CERT-EU-2021-067 GHSA-8489-44mv-ggj8					
	cpe:/a:apache:log4j [2.13.0, 2.17.1), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.17.1)					
`CVE-2021-44228`	10.0		Critical		Escalate	In Review
	CERT-EU-2021-070, CERT-EU-2021-075, CERT-EU-2021-072, CERT-EU-2022-005, CERT-EU-2021-074, CERT-EU-2021-073, CERT-EU-2021-067, CERT-EU-2021-071, CERT-EU-2021-076 GHSA-jfh8-c2jp-5v3q					
	cpe:/a:apache:log4j [2.13.0, 2.15.0), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.15.0)					

Table 1: log4j-core Vulnerabilities

log4j-api

Artifacts

Component	Artifact Id	Version
log4j-api	`log4j-api-2.14.0.jar`	`2.14.0`

Vulnerabilities

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
CVE-2021-45105	5.9		Medium		Due	Insignificant
	CERT-EU-2021-067 GHSA-p6xc-xr62-6r2g					
	cpe:/a:apache:log4j [2.13.0, 2.16.0], GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.17.0)					
CVE-2021-45046	9.0		Critical		Escalate	In Review
	CERT-EU-2021-075, CERT-EU-2021-067, CERT-EU-2021-076 GHSA-7rjr-3q55-vv33					
	cpe:/a:apache:log4j [2.13.0, 2.16.0), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.16.0)					
CVE-2021-44832	6.6		Medium		Default	Insignificant
	CERT-EU-2021-067 GHSA-8489-44mv-ggj8					
	cpe:/a:apache:log4j [2.13.0, 2.17.1), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.17.1)					
CVE-2021-44228	10.0		Critical		Escalate	In Review
	CERT-EU-2021-070, CERT-EU-2021-075, CERT-EU-2021-072, CERT-EU-2022-005, CERT-EU-2021-074, CERT-EU-2021-073, CERT-EU-2021-067, CERT-EU-2021-071, CERT-EU-2021-076 GHSA-jfh8-c2jp-5v3q					
	cpe:/a:apache:log4j [2.13.0, 2.15.0), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.15.0)					

Table 2: log4j-api Vulnerabilities

5 example Vulnerability Notice

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

6 example Vulnerability List

The following vulnerabilities have been identified and categorized.

Applicable

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

In Review

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

Name	Score	Score$_{ctx}$	Severity	Severity$_{ctx}$	Priority	Status
CVE-2021-44228	10.0		Critical		Escalate	In Review
	CERT-EU-2021-070, CERT-EU-2021-075, CERT-EU-2021-072, CERT-EU-2022-005, CERT-EU-2021-074, CERT-EU-2021-073, CERT-EU-2021-067, CERT-EU-2021-071, CERT-EU-2021-076 GHSA-jfh8-c2jp-5v3q					
	cpe:/a:apache:log4j [2.13.0, 2.15.0), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.15.0)					
CVE-2022-22965	9.8		Critical		Escalate	In Review
	CERT-EU-2022-023 GHSA-36p3-wjmg-h94x					
	GHSA org.springframework:spring-beans (Maven) [5.3.0, 5.3.18)					
CVE-2021-45046	9.0		Critical		Escalate	In Review
	CERT-EU-2021-075, CERT-EU-2021-067, CERT-EU-2021-076 GHSA-7rjr-3q55-vv33					
	cpe:/a:apache:log4j [2.13.0, 2.16.0), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.16.0)					

Table 3: In Review Category (example)

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-2021-44832	6.6		Medium		Default	Insignificant
	CERT-EU-2021-067 GHSA-8489-44mv-ggj8					
	cpe:/a:apache:log4j [2.13.0, 2.17.1), GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.17.1)					
CVE-2023-20863	6.5		Medium		Default	Insignificant
	GHSA-wxqc-pxw9-g2p8					
	GHSA org.springframework:spring-expression (Maven) [5.3.0, 5.3.27)					
CVE-2023-20861	6.5		Medium		Default	Insignificant
	GHSA-564r-hj7v-mcr5					
	GHSA org.springframework:spring-expression (Maven) [5.3.0, 5.3.26)					
CVE-2022-22950	6.5		Medium		Default	Insignificant
	GHSA-558x-2xjg-6232					

Name	Score	Score$_{\text{ctx}}$	Severity	Severity$_{\text{ctx}}$	Priority	Status
	GHSA org.springframework:spring-expression (Maven) [5.3.0, 5.3.17)					
CVE-2021-45105	5.9		Medium		Due	Insignificant
	CERT-EU-2021-067 GHSA-p6xc-xr62-6r2g					
	cpe:/a:apache:log4j [2.13.0, 2.16.0], GHSA org.apache.logging.log4j:log4j-core (Maven) [2.13.0, 2.17.0)					
CVE-2024-38820	5.3		Medium		Default	Insignificant
	GHSA-4gc7-5j7h-4qph					
	GHSA org.springframework:spring-context (Maven) [0, 6.1.14)					
CVE-2022-22970	5.3		Medium		Default	Insignificant
	GHSA-hh26-6xwr-ggv7					
	GHSA org.springframework:spring-beans (Maven) [5.3.0, 5.3.20)					
CVE-2022-22968	5.3		Medium		Default	Insignificant
	GHSA-g5mm-vmx4-3rg7					
	GHSA org.springframework:spring-context (Maven) [5.3.0, 5.3.19)					
CVE-2024-38808	5.1		Medium		Default	Insignificant
	GHSA-9cmq-m9j5-mvww					
	GHSA org.springframework:spring-expression (Maven) [0, 5.3.39)					

Table 4: Insignificant Category (example)

Void

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