Gestione delle Vulnerabilità

Release 3.3.13

Link.it

26 giu 2023

Indice

Introduzione

Le potenziali vulnerabilità sono gestite nel progetto GovWay in accordo a processi rigorosi e documentati. La segnalazione di una potenziale vulnerabilità può avvenire tramite diverse fonti:

- l'analisi delle librerie terza parte, descritta nella sezione releaseProcessGovWay_thirdPartyDynamicAnalysis_ci, rileva una vulnerabilità tramite il tool OWASP Dependency-Check;

- i test di sicurezza, descritti nella sezione releaseProcessGovWay_dynamicAnalysis_security, rilevano un nuovo problema o una regressione;

- dagli utenti di GovWay tramite l'apertura di un GovWay Issue.

Qualunque sia la provenienza, la segnalazione viene immediatamente analizzata al fine di verificare:

- se si tratta di un falso positivo e in tal case registrarlo come tale: *Falsi Positivi*;

- se si tratta di una vulnerabilità con un effettivo impatto sul software GovWay; in tal caso viene registrato un nuovo avviso di sicurezza ed avviato il processo di risoluzione, così come descritto nella sezione *Avvisi di Sicurezza*.

Avvisi di Sicurezza

Le vulnerabilità sono classificate per severità rispetto al CVSS 3.1 scoring system sintetizzato dalla tabella riportata nella figura Fig. 2.1.

Fig. 2.1: CVSS 3.1 scoring system

Tempi di Risoluzione

Le tempistiche di risoluzione delle vulnerabilità sono classificate rispetto alla loro severità e garantite per le versioni Enterprise del prodotto. Per la versione community i fix saranno applicati sulle prime versioni in rilascio. In caso di vulnerabilità molto impattanti saranno prodotte patch version immediate anche per le versioni community.

I tempi sono calcolati rispetto alla data di identificazione dell'impatto della vulnerabilità sul prodotto (true positive).

Tabella 2.1: Avvisi di Sicurezza: tempi di risoluzione

Severità (CSSS Score)	Tempistica	Fix Version
Critical (9.0-10.0)	10 giorni	Patch version
High (7.0-8.9)	20 giorni	Patch version

Tabella 2.1 – continua dalla pagina precedente

Severità (CSSS Score)	Tempistica	Fix Version
Medium (4.0 - 6.9)	45 giorni	Patch o Minor version
Low (3.9 or below)	n.d.	A discrezione del progetto

Elenco degli Avvisi

Gli avvisi vengono classificati per anno di registrazione:

- *Avvisi di Sicurezza 2022*
- *Avvisi di Sicurezza 2021*

2.1 Avvisi di Sicurezza 2023

- *CVE-2023-33201*
- *CVE-2017-9096*
- *CVE-2022-24196 e CVE-2022-24197*
- *CVE-2023-34411*
- *CVE-2023-33264*
- *CVE-2023-20862*
- *CVE-2023-20863*
- *CVE-2022-42003*
- *CVE-2023-20861*
- *CVE-2023-1436*
- *CVE-2023-1370*
- *CVE-2020-8908*
- *CVE-2023-24998*
- *CVE-2022-45688*

2.1.1 CVE-2023-33201

Data: 2023-06-20

Severity: Medium

CVSS Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

Riferimenti: https://github.com/bcgit/bc-java/wiki/CVE-2023-33201

Libreria: org.bouncycastle:bcprov-ext-jdk18on < 1.74

Descrizione

The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms. This jar contains JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.8 and up. Note: this package includes the NTRU encryption algorithms.

GovWay

Versione affette: <= 3.3.12

Risoluzione: 3.3.13

2.1.2 CVE-2017-9096

Data: 2023-06-15

Severity: High

CVSS Score: 8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2017-9096

Libreria: com.lowagie:itext < 5.5.12

Descrizione

The XML parsers in iText before 5.5.12 and 7.x before 7.0.3 do not disable external entities, which might allow remote attackers to conduct XML external entity (XXE) attacks via a crafted PDF.

GovWay

Versione affette: <= 3.3.12

Risoluzione: 3.3.13

2.1.3 CVE-2022-24196 e CVE-2022-24197

Data: 2023-06-15

Severity: Medium

CVSS Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

Riferimenti:

- https://nvd.nist.gov/vuln/detail/CVE-2022-24196
- https://nvd.nist.gov/vuln/detail/CVE-2022-24197

Libreria: com.lowagie:itext < 7.1.17

Descrizione

- CVE-2022-24196: iText v7.1.17, up to (exluding)»: 7.1.18 and 7.2.2 was discovered to contain an out-of-memory error via the component readStreamBytesRaw, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.
- CVE-2022-24197: iText v7.1.17 was discovered to contain a stack-based buffer overflow via the component ByteBuffer.append, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.

GovWay

Versione affette: <= 3.3.12

Risoluzione: 3.3.13

2.1.4 CVE-2023-34411

Data: 2023-06-14

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2023-34411

Libreria: com.fasterxml.woodstox:woodstox-core <= 6.4.0

Descrizione

The xml-rs crate before 0.8.14 for Rust and Crab allows a denial of service (panic) via an invalid <! token (such as <!DOCTYPEs/%<!A nesting) in an XML document. The earliest affected version is 0.8.9.

GovWay

Versione affette: <= 3.3.12

Risoluzione: 3.3.13

2.1.5 CVE-2023-33264

Data: 2023-05-23

Severity: Medium

CVSS Score: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2023-33264

Libreria: com.hazelcast:hazelcast < 5.3.0

Descrizione

In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, configuration routines don't mask passwords in the member configuration properly. This allows Hazelcast Management Center users to view some of the secrets.

GovWay

Versione affette: <= 3.3.12

Risoluzione: 3.3.13

2.1.6 CVE-2023-20862

Data: 2023-04-20

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2023-20862

Libreria: org.springframework.security:spring-security-* < 5.7.8

Descrizione

In Spring Security, versions 5.7.x prior to 5.7.8, versions 5.8.x prior to 5.8.3, and versions 6.0.x prior to 6.0.3, the logout support does not properly clean the security context if using serialized versions. Additionally, it is not possible to explicitly save an empty security context to the HttpSessionSecurityContextRepository. This vulnerability can keep

users authenticated even after they performed logout. Users of affected versions should apply the following mitigation. 5.7.x users should upgrade to 5.7.8. 5.8.x users should upgrade to 5.8.3. 6.0.x users should upgrade to 6.0.3.

GovWay

Versione affette: <= 3.3.12

Risoluzione: 3.3.13

2.1.7 CVE-2023-20863

Data: 2023-04-16

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

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

Libreria: org.springframework:spring-expression <= 5.3.26

Descrizione

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.

GovWay

Versione affette: <= 3.3.11

Risoluzione: 3.3.12

2.1.8 CVE-2022-42003

Data: 2023-04-04

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-42003

Libreria: com.fasterxml.jackson.core:jackson-databind <= 2.13.4.1

Descrizione

In FasterXML jackson-databind before 2.14.0-rc1, resource exhaustion can occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled. Additional fix version in 2.13.4.1 and 2.12.17.1

GovWay

Versione affette: <= 3.3.11

Risoluzione: 3.3.12

2.1.9 CVE-2023-20861

Data: 2023-03-29

Severity: Medium

CVSS Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

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

Libreria: org.springframework:spring-* <= 5.3.25

Descrizione

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.

GovWay

Versione affette: <= 3.3.11

Risoluzione: 3.3.12

2.1.10 CVE-2023-1436

Data: 2023-03-18

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://ossindex.sonatype.org/vulnerability/CVE-2023-1436

Libreria: org.codehaus.jettison:jettison <= 1.5.3

Descrizione

CWE-400: Uncontrolled Resource Consumption ("Resource Exhaustion")

jettison - Denial of Service (DoS)

GovWay

Versione affette: <= 3.3.11

Risoluzione: 3.3.12

2.1.11 CVE-2023-1370

Data: 2023-03-18

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://ossindex.sonatype.org/vulnerability/CVE-2023-1370

Libreria: net.minidev:json-smart <= 2.4.8

Descrizione

CWE-400: Uncontrolled Resource Consumption ("Resource Exhaustion")

json-smart - Denial of Service (DoS)

GovWay

Versione affette: <= 3.3.11

Risoluzione: 3.3.12

2.1.12 CVE-2020-8908

Data: 2023-03-08

Severity: Low

CVSS Score: 3.3 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2020-8908

Libreria: com.google.guava:guava <= 31.1-jre

Descrizione

A temp directory creation vulnerability exists in all versions of Guava, allowing an attacker with access to the machine to potentially access data in a temporary directory created by the Guava API com.google.common.io.Files.createTempDir(). By default, on unix-like systems, the created directory is world-readable (readable by an attacker with access to the system). The method in question has been marked @Deprecated in versions 30.0 and later and should not be used. For Android developers, we recommend choosing a temporary directory API provided by Android, such as context.getCacheDir(). For other Java developers, we recommend migrating to the Java 7 API java.nio.file.Files.createTempDirectory() which explicitly configures permissions of 700, or configuring the Java runtime's java.io.tmpdir system property to point to a location whose permissions are appropriately configured.

GovWay

Versione affette: <= 3.3.10

Risoluzione: 3.3.13

2.1.13 CVE-2023-24998

Data: 2023-02-22

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2023-24998

Libreria: commons-fileupload:commons-fileupload <= 1.4

Descrizione

Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads.

GovWay

Versione affette: <= 3.3.10

Risoluzione: 3.3.11

2.1.14 CVE-2022-45688

Data: 2023-02-06

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-45688

Libreria: org.json:json <= 20220924

Descrizione

A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.

GovWay

Versione affette: <= 3.3.10

Risoluzione: 3.3.11

2.2 Avvisi di Sicurezza 2022

- *CVE-2022-46364*
- *CVE-2022-41915*
- *CVE-2021-37533*
- *CVE-2022-40150*
- *CVE-2022-[40152-40156]*
- *CVE-2022-31692*
- *CVE-2022-34169*
- *CVE-2021-44832*

2.2.1 CVE-2022-46364

Data: 2022-12-14

Severity: Critical

CVSS Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-46364

Libreria: org.apache.cxf:cxf-core >= 3.5.0, < 3.5.5

Descrizione

A SSRF vulnerability in parsing the href attribute of XOP:Include in MTOM requests in versions of Apache CXF before 3.5.5 and 3.4.10 allows an attacker to perform SSRF style attacks on webservices that take at least one parameter of any type.

GovWay

Versione affette: <= 3.3.9.p3

Risoluzione: 3.3.10

2.2.2 CVE-2022-41915

Data: 2022-12-14

Severity: Medium

CVSS Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-41915

Libreria: io.netty:netty-codec < 4.1.86.Final

Descrizione

Netty project is an event-driven asynchronous network application framework. In versions prior to 4.1.86.Final, when calling *DefaultHttpHeadesr.set* with an _iterator_ of values, header value validation was not performed, allowing malicious header values in the iterator to perform HTTP Response Splitting. This issue has been patched in version 4.1.86.Final. Integrators can work around the issue by changing the *DefaultHttpHeaders.set(CharSequence, Iterator<?>)* call, into a *remove()* call, and call *add()* in a loop over the iterator of values.

GovWay

Versione affette: <= 3.3.9.p3

Risoluzione: 3.3.10

2.2.3 CVE-2021-37533

Data: 2022-12-07

Severity: Medium

CVSS Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2021-37533

Libreria: apache:commons_net <= 3.8.0

Descrizione

Prior to Apache Commons Net 3.9.0, Net's FTP client trusts the host from PASV response by default. A malicious server can redirect the Commons Net code to use a different host, but the user has to connect to the malicious server in the first place. This may lead to leakage of information about services running on the private network of the client. The default in version 3.9.0 is now false to ignore such hosts, as cURL does. See https://issues.apache.org/jira/browse/NET-711.

GovWay

Nota: GovWay non utilizza il codice che possiede la vulnerabilità.

Versione affette: <= 3.3.9.p2

Risoluzione: 3.3.9.p3

2.2.4 CVE-2022-40150

Data: 2022-12-03

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-40150

Libreria: jettison_project:jettison <= 1.5.1

Descrizione

Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by Out of memory. This effect may support a denial of service attack.

GovWay

Versione affette: <= 3.3.9.p2

Risoluzione: 3.3.9.p3

2.2.5 CVE-2022-[40152-40156]

Data: 2022-10-28

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti:

- https://nvd.nist.gov/vuln/detail/CVE-2022-40152
- https://nvd.nist.gov/vuln/detail/CVE-2022-40153
- https://nvd.nist.gov/vuln/detail/CVE-2022-40154
- https://nvd.nist.gov/vuln/detail/CVE-2022-40155
- https://nvd.nist.gov/vuln/detail/CVE-2022-40156

Libreria: com.fasterxml.woodstox:woodstox-core >= 6.0.0, < 6.4.0

Descrizione

Those using Xstream to seralize XML data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack.

GovWay

Versione affette: <= 3.3.8

Risoluzione: 3.3.9

2.2.6 CVE-2022-31692

Data: 2022-10-29

Severity: Critical

CVSS Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-31692

Libreria: org.springframework.security:spring-security-core >= 5.7.0, < 5.7.5

Descrizione

Spring Security, versions 5.7 prior to 5.7.5 and 5.6 prior to 5.6.9 could be susceptible to authorization rules bypass via forward or include dispatcher types. Specifically, an application is vulnerable when all of the following are true: The application expects that Spring Security applies security to forward and include dispatcher types. The application uses the AuthorizationFilter either manually or via the authorizeHttpRequests() method. The application configures the FilterChainProxy to apply to forward and/or include requests (e.g. spring.security.filter.dispatcher-types = request, error, async, forward, include). The application may forward or include the request to a higher privilege-secured endpoint.The application configures Spring Security to apply to every dispatcher type via authorizeHttpRequests().shouldFilterAllDispatcherTypes(true)

GovWay

Versioni affette: <= 3.3.8

Risoluzione: 3.3.9

2.2.7 CVE-2022-34169

Data: 2022-10-27

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-34169

Libreria: xalan:xalan <= 2.7.2

Descrizione

The Apache Xalan Java XSLT library is vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode. The Apache Xalan Java project is dormant and in the process of being retired. No future releases of Apache Xalan Java to address this issue are expected. Note: Java runtimes (such as OpenJDK) include repackaged copies of Xalan.

A fix for this issue was published in September 2022 as part of an anticipated 2.7.3 release.

GovWay

Versione affette: <= 3.3.8

Risoluzione: 3.3.9

2.2.8 CVE-2021-44832

Data: 2022-01-04

Severity: Medium

CVSS Score: 6.6 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

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

Libreria: org.apache.logging.log4j:log4j-core <= 2.17.0

Descrizione

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.

GovWay

Versioni affette: <= 3.3.5.p2

Risoluzione: 3.3.6

2.3 Avvisi di Sicurezza 2021

- *CVE-2021-45105*
- *CVE-2021-45046*
- *CVE-2021-44228*

2.3.1 CVE-2021-45105

Data: 2021-12-20

Severity: Medium

CVSS Score: 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

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

Libreria: org.apache.logging.log4j:log4j-core <= 2.16.0

Descrizione

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.

GovWay

Versioni affette: <= 3.3.5.p2

Risoluzione: 3.3.6

2.3.2 CVE-2021-45046

Data: 2021-12-11

Severity: Critical

CVSS Score: 9.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

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

Libreria: org.apache.logging.log4j:log4j-core <= 2.15.0

Descrizione

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.

GovWay

Versioni affette: <= 3.3.5.p1

Risoluzione: 3.3.5.p2

2.3.3 CVE-2021-44228

Data: 2021-12-07

Severity: Critical

CVSS Score: 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

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

Libreria: org.apache.logging.log4j:log4j-core <= 2.14.1

Descrizione

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.

GovWay

Versioni affette: <= 3.3.5

Risoluzione: 3.3.5.p1

Falsi Positivi

- *CVE-2023-35116*
- *CVE-2022-42920*
- *CVE-2022-40705*
- *CVE-2022-45688*
- *CVE-2021-37533*
- *CVE-2020-5408*
- *CVE-2022-0869*
- *CVE-2022-[38752,41854,1471,3064] CVE-2021-4235*
- *CVE-2017-10355*
- *CVE-2016-1000027*

3.1 CVE-2023-35116

Data: 2023-06-21

Severity: High

CVSS Score: -

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2023-35116

Libreria: com.fasterxml.jackson.core:jackson-databind <= 2.14.2

Descrizione

** DISPUTED ** An issue was discovered jackson-databind thru 2.15.2 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies. NOTE: the vendor's perspective is that the product is not intended for use with untrusted input.

Falso Positivo per GovWay

Il progetto "FasterXML" ha dichiarato l'issue un falso positivo nell'issue 3972.

Configuration File: false-positive.xml

3.2 CVE-2022-42920

Data: 2023-03-09

Severity: Critical

CVSS Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-42920

Libreria: org.apache.bcel:bcel < 6.6.0

Descrizione

Apache Commons BCEL has a number of APIs that would normally only allow changing specific class characteristics. However, due to an out-of-bounds writing issue, these APIs can be used to produce arbitrary bytecode. This could be abused in applications that pass attacker-controllable data to those APIs, giving the attacker more control over the resulting bytecode than otherwise expected. Update to Apache Commons BCEL 6.6.0.

Falso Positivo per GovWay

La libreria non viene inclusa in GovWay e quindi la segnalazione è considerabile un falso positivo.

Configuration File: false-positive.xml

3.3 CVE-2022-40705

Data: 2023-03-09

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-40705

Libreria: soap:soap >= 2.2

Descrizione

An Improper Restriction of XML External Entity Reference vulnerability in RPCRouterServlet of Apache SOAP allows an attacker to read arbitrary files over HTTP. This issue affects Apache SOAP version 2.2 and later versions. It is unknown whether previous versions are also affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

Falso Positivo per GovWay

La libreria vulnerabile non viene utilizzata in GovWay e quindi la segnalazione è considerabile un falso positivo.

Il faso positivo è stato segnalato nell'issue 5543 del tool OWASP Dependency-Check.

Configuration File: false-positive.xml

3.4 CVE-2022-45688

Data: 2023-02-28

Severity: High

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-45688

Libreria: org.json:json <= 20220924

Descrizione

A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.

Falso Positivo per GovWay

La versione utilizzata in GovWay è superiore alla "20220924" quindi la segnalazione è considerabile un falso positivo.

La vulnerabilità è stata risolta nella versione "20230227" come descritto nell'issue 708 e nella pull request 720.

Configuration File: false-positive.xml

3.5 CVE-2021-37533

Data: 2023-02-22

Severity: Medium

CVSS Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2021-37533

Libreria: commons-net:commons-net < 3.9.0

Descrizione

Prior to Apache Commons Net 3.9.0, Net's FTP client trusts the host from PASV response by default. A malicious server can redirect the Commons Net code to use a different host, but the user has to connect to the malicious server in the first place. This may lead to leakage of information about services running on the private network of the client. The default in version 3.9.0 is now false to ignore such hosts, as cURL does. See https://issues.apache.org/jira/browse/NET-711.

Falso Positivo per GovWay

La segnalazione avviene poichè alcune delle librerie utilizzate in GovWay richiedono come dipendenza transitiva delle versioni della libreria vulnerabili. In GovWay viene però inclusa la versione commons-net-3.9.0.jar che non presenta la vulnerabilità e quindi la segnalazione è considerabile un falso positivo.

Configuration File: false-positive.xml

3.6 CVE-2020-5408

Data: 2022-11-14

Severity: Medium

CVSS Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2020-5408

Libreria: org.springframework.security:spring-security-crypto <= 5.3.2

Descrizione

Spring Security versions 5.3.x prior to 5.3.2, 5.2.x prior to 5.2.4, 5.1.x prior to 5.1.10, 5.0.x prior to 5.0.16 and 4.2.x prior to 4.2.16 use a fixed null initialization vector with CBC Mode in the implementation of the queryable text encryptor. A malicious user with access to the data that has been encrypted using such an encryptor may be able to derive the unencrypted values using a dictionary attack.

Falso Positivo per GovWay

La versione utilizzata in GovWay è superiore alla "5.3.2" quindi la segnalazione è considerabile un falso positivo.

Dalle discussioni degli issues 287 e 284 del repository "OSSIndex" si possono comprendere i motivi della segnalazione: nelle versioni precedenti alla 6.x spring-security ha solamente deprecato l'utilizzo degli oggetti vulnerabili. Nel progetto GovWay comunque il metodo oggetto della vulnerabilità (Encryptors#queryableText(CharSequence, CharSequence)) non viene utilizzato.

Configuration File: false-positive.xml

3.7 CVE-2022-0869

Data: 2022-11-14

Severity: Medium

CVSS Score: 6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2022-0869

Libreria: commons-discovery:commons-discovery 0.5

Descrizione

Multiple Open Redirect in GitHub repository nitely/spirit prior to 0.12.3.

Falso Positivo per GovWay

Non risultano vulnerabilità note relative alla libreria commons-discovery (verifica effettuata tramite sonatype).

Viene descrito come un falso positivo anche nell'issuer Issue 4644 del plugin OWASP Dependency-Check.

Configuration File: false-positive.xml

3.8 CVE-2022-[38752,41854,1471,3064] CVE-2021-4235

Data: 2022-10-10

Severity: High/Medium

CVSS Score: 7.5, 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

Riferimenti:

- https://nvd.nist.gov/vuln/detail/CVE-2022-38752
- https://nvd.nist.gov/vuln/detail/CVE-2022-41854
- https://nvd.nist.gov/vuln/detail/CVE-2022-1471
- https://nvd.nist.gov/vuln/detail/CVE-2022-3064
- https://nvd.nist.gov/vuln/detail/CVE-2021-4235

Libreria: org.yaml:snakeyaml 1.33

Descrizione

- CVE-2022-38752: Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack-overflow.

- CVE-2022-41854: Those using Snakeyaml to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack overflow. This effect may support a denial of service attack.

- CVE-2022-1471: SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization.

- CVE-2022-3064: Parsing malicious or large YAML documents can consume excessive amounts of CPU or memory.

- CVE-2021-4235: Due to unbounded alias chasing, a maliciously crafted YAML file can cause the system to consume significant system resources. If parsing user input, this may be used as a denial of service vector.

Falso Positivo per GovWay

Le vulnerabilità non sono sfruttabili su GovWay per effettuare attacchi poichè la libreria viene utilizzata solamente per la gestione delle interfacce yaml caricate sulla console dagli amministratori e non viene utilizzata per input forniti dinamicamente nelle richieste gestite dai componenti di runtime.

Configuration File: false-positive.xml

3.9 CVE-2017-10355

Data: 2022-08-14

Severity: Medium

CVSS Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2017-10355

Libreria: xerces:xercesImpl 2.12.2

Descrizione

Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

Falso Positivo per GovWay

La vulnerabilità "CVE-2017-10355" è oggetto di discussione e aperture di segnalazioni poichè non presente nel database nvd.nist.gov ma invece rilevata da Sonatype OSSIndex come si evince dalle discussioni degli issues 4614 e 316: «the intelligence that this CVE (still) applies to version 2.12.2 comes from the security analysts of Sonatype OSSINDEX, not from the NVD datastreams».

In particolare la vulnerabilità sonatype-2017-0348 non ha poi una evidenza nel blog esistente (il link https://blogs.securiteam.com/index.php/archives/3271 non esiste). Il contenuto del blog può essere recuperato esaminando l'issue 4614 nel quale sembra che la problematica rilevata fosse sul metodo XMLEntityManager.setupCurrentEntity() che non dispone di un meccanismo di timeout; il metodo non viene utilizzato su GovWay.

Nella discussione si fa inoltre riferimento alla vulnerabilità descritta in SNYK-JAVA-XERCES-31497 che consentiva di attuare attacchi DOS. Nel progetto GovWay è comunque corretto considerarlo un falso positivo poichè la libreria viene utilizzata per espressioni xpath configurate solamente sulla console dagli amministratori e non fornite in input dinamicamente nelle richieste gestite dai componenti runtime. Infine su GovWay è disabilitato l'accesso a risorse esterne (DTDs.enabled=false).

Configuration File: false-positive.xml

3.10 CVE-2016-1000027

Data: 2022-08-10

Severity: Critical

CVSS Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Riferimenti: https://nvd.nist.gov/vuln/detail/CVE-2016-1000027

Libreria: org.springframework:spring-web <= 5.3.16

Descrizione

Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

Falso Positivo per GovWay

La versione della libreria utilizzata in GovWay è superiore alla "5.3.16" quindi la segnalazione è considerabile un falso positivo.

Dalle discussioni degli issues 4849 e 4558 del plugin OWASP Dependency-Check si possono comprendere i motivi della segnalazione: nelle versioni precedenti alla 6.x spring ha solamente deprecato l'utilizzo degli oggetti vulnerabili. Nel progetto GovWay comunque la classe oggetto della vulnerabilità (remoting-httpinvoker) non viene utilizzata.

Configuration File: false-positive.xml