



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)



[Sponsor](#)

## Project: project ':designer'

clear-reports:designer:23.10

Scan Information ([show all](#)):

- *dependency-check version*: 7.4.4
- *Report Generated On*: Tue, 16 Jan 2024 13:36:17 +0100
- *Dependencies Scanned*: 222 (195 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 16
- ...

## Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
------------	-------------------	---------	------------------	-----------	------------	----------------

## Dependencies

## Suppressed Vulnerabilities



**datasource.cassandra.zip: native-protocol.jar**

### Description:

A set of Java types representing the frames and messages of the Apache Cassandra® native protocol, with the associated serialization and deserialization logic (this is a third-party implementation, not related to the Apache Cassandra project)

### License:

Apache 2: <http://www.apache.org/licenses/LICENSE-2.0.txt>

**File Path:** /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/designer/build/tmp/dependencies/i-net Clear Reports Designer/plugins/datasource.cassandra.zip/native-protocol.jar

**MD5:** 3c4bf24fd592b01cff5234428080230d

SHA1: 97e812373a5fe7667384e7ad67819d2c71878bf8

SHA256: 955120805ddadd0771b36124679e337a20959c5639bc5de82bb8bce96b10441e

#### Evidence



#### Suppressed Identifiers

- None

#### Suppressed Vulnerabilities



##### [CVE-2020-13946](#) suppressed

In Apache Cassandra, all versions prior to 2.1.22, 2.2.18, 3.0.22, 3.11.8 and 4.0-beta2, it is possible for a local attacker without access to the Apache Cassandra process or configuration files to manipulate the RMI registry to perform a man-in-the-middle attack and capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and perform unauthorised operations. Users should also be aware of CVE-2019-2684, a JRE vulnerability that enables this issue to be exploited remotely.

CWE-668 Exposure of Resource to Wrong Sphere

Notes: Possible false positive, since the CVE is a year old and it does not match this package and version file name: datasource.cassandra.zip: native-protocol.jar

##### CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

##### CVSSv3:

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

##### References:

- - [\[cassandra-user\] 20200901 Re: CVE-2020-13946 Apache Cassandra RMI Rebind Vulnerability](#)
- - [\[cassandra-user\] 20200902 Re: CVE-2020-13946 Apache Cassandra RMI Rebind Vulnerability](#)
- - [\[cassandra-user\] 20200911 Re: CVE-2020-13946 Apache Cassandra RMI Rebind Vulnerability](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20210521-0005/>
- MISC - <https://lists.apache.org/thread.html/rcd7544b24d8fc32b7950ec4c117052410b661babaa857fb1fc641152%40%3Cuser.cassandra.apache.org%3E>

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:cassandra:\\*:\\*:\\*:\\*:\\* versions up to \(excluding\) 2.1.22](#)
- ...

facturx.zip: jakarta.activation-api.jar

#### Description:

\${project.name} \${spec.version} Specification

#### License:

EDL 1.0: <http://www.eclipse.org/org/documents/edl-v10.php>

**File Path:** /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/designer/build/tmp/dependencies/i-net Clear Reports Designer/plugins/facturx.zip/jakarta.activation-api.jar

**MD5:** 1af11450fafc7ee26c633d940286bc16

**SHA1:** 640c0d5aff45dbff1e1a1bc09673ff3a02b1ba12

**SHA256:** f53f578dd0eb4170c195a4e215c59a38abfb4123dcb95dd902fef92876499fbb

#### Evidence

#### Suppressed Identifiers

- None

#### Suppressed Vulnerabilities

##### [CVE-2023-4218](#) suppressed

In Eclipse IDE versions < 2023-09 (4.29) some files with xml content are parsed vulnerable against all sorts of XXE attacks. The user just needs to open any evil project or update an open project with a vulnerable file (for example for review a foreign repository or patch).

CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2019-10799 - This is for the project compile-sass and not the used sass-compiler. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is stupid CVE for a sample python project. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-4218 - This is for the eclipse ide and not for any library from eclipse. CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core.

CVSSv3:

- MEDIUM (5.0)
- CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

References:

- <https://github.com/eclipse-cdt/cdt/commit/c7169b3186d2fef20f97467c3e2ad78e2943ed1b>
- <https://github.com/eclipse-emf/org.eclipse.emf/issues/10>
- <https://github.com/eclipse-jdt/eclipse.jdt.core/commit/38dd2a878f45cdb3d8d52090f1d6d1b532fd4c4d>
- <https://github.com/eclipse-jdt/eclipse.jdt.ui/commit/13675b1f8a74f47de4da89ed0ded6af7c21dfbec>
- <https://github.com/eclipse-pde/eclipse.pde/pull/632/>
- <https://github.com/eclipse-pde/eclipse.pde/pull/667/>
- <https://github.com/eclipse-platform/eclipse.platform.releng.buildtools/pull/45>
- <https://github.com/eclipse-platform/eclipse.platform.swt/commit/bf71db5ddcb967c0863dad4745367b54f49e06ba>
- <https://github.com/eclipse-platform/eclipse.platform.ui/commit/f243cf0a28785b89b7c50bf4e1cce48a917d89bd>
- <https://github.com/eclipse-platform/eclipse.platform/pull/761>
- <https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/8>

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:eclipse:eclipse\\_ide:\\*:\\*:\\*:\\*:\\* versions up to \(excluding\) 4.29](#)
- ...

#### [CVE-2008-7271](#) suppressed

Multiple cross-site scripting (XSS) vulnerabilities in the Help Contents web application (aka the Help Server) in Eclipse IDE, possibly 3.3.2, allow remote attackers to inject arbitrary web script or HTML via (1) the searchWord parameter to help/advanced/searchView.jsp or (2) the workingSet parameter in an add action to help/advanced/workingSetManager.jsp, a different issue than CVE-2010-4647.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2019-10799 - This is for the project compile-sass and not the used sass-compiler. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is stupid CVE for a sample phyton project. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-4218 - This is for the eclipse ide and not for any library from eclipse. CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core.

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

References:

- MISC - <http://r00tin.blogspot.com/2008/04/eclipse-local-web-server-exploitation.html>
- MISC - [https://bugs.eclipse.org/bugs/show\\_bug.cgi?id=223539](https://bugs.eclipse.org/bugs/show_bug.cgi?id=223539)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:eclipse:eclipse\\_ide:\\*:\\*:\\*:\\*:\\*](#)
- ...

#### [CVE-2010-4647](#) suppressed

Multiple cross-site scripting (XSS) vulnerabilities in the Help Contents web application (aka the Help Server) in Eclipse IDE before 3.6.2 allow remote attackers to inject arbitrary web script or HTML via the query string to (1) help/index.jsp or (2) help/advanced/content.jsp.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2019-10799 - This is for the project compile-sass and not the used sass-compiler. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is stupid CVE for a sample phyton project. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-4218 - This is for the eclipse ide and not for any library from eclipse. CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core.

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

References:

- FEDORA - [FEDORA-2010-18990](#)
- FEDORA - [FEDORA-2010-19006](#)
- MANDRIVA - [MDVSA-2011:032](#)

- MISC - [http://yehg.net/lab/pr0js/advisories/eclipse/%5Beclipse\\_help\\_server%5D\\_cross\\_site\\_scripting](http://yehg.net/lab/pr0js/advisories/eclipse/%5Beclipse_help_server%5D_cross_site_scripting)
- MISC - [https://bugs.eclipse.org/bugs/show\\_bug.cgi?id=329582](https://bugs.eclipse.org/bugs/show_bug.cgi?id=329582)
- MLIST - [\[oss-security\] 20110106 CVE Request: Eclipse IDE Version: 3.6.1 | Help Server Local Cross Site Scripting \(XSS\)](#)
- MLIST - [\[oss-security\] 20110106 Re: CVE Request: Eclipse IDE Version: 3.6.1 | Help Server Local Cross Site Scripting \(XSS\)](#)
- REDHAT - [RHSA-2011:0568](#)
- XF - [eclipseide-querystring-xss\(64833\)](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:eclipse:eclipse\\_ide:\\*:\\*:\\*:\\*:\\* versions up to \(including\) 3.6.1](#)
- ...

## reporting.zip: reporting-javadoc.jar: jquery-ui.js

**File Path:** /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/designer/build/tmp/dependencies/i-net Clear Reports Designer/plugins/reporting.zip/reporting-javadoc.jar/jquery/jquery-ui.js

**MD5:** 3e34f50eab2e13d720c93e44ac5cb7ca

**SHA1:** c432ac324c727a86a9a54eff1b90d79e115e3f16

**SHA256:** 712e2e2efe1717a1e10aee0e02163e1deadf88760ade58b5cdfc333ea6de5247

### Evidence



### Related Dependencies



### Suppressed Identifiers

- None

### Suppressed Vulnerabilities



[CVE-2021-41182](#) suppressed

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the DatePicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: Javadoc embedded JQuery UI - requires updated Java Version with newer javadoc

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:

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

## References:

- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20211118-0004/>
- CONFIRM - <https://www.drupal.org/sa-core-2022-002>
- CONFIRM - <https://www.tenable.com/security/tns-2022-09>
- MISC - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
- MISC - <https://github.com/jquery/jquery-ui/pull/1954/commits/6809ce843e5ac4128108ea4c15cbc100653c2b63>
- MISC - <https://lists.debian.org/debian-lts-announce/2023/08/msg00040.html>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/HVKIOWSXL2RF2ULNAP7PHESYCFSTIJE3/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/NXIUUBRVL4E7G7MMIKCEN75YN7UFERW/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/O74SXY7RGXREQDQUDQD4BPJ4QQTD2XQ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SGSY236PYSFYIEBRGDERLA7OSY6D7XL4/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SNXA7XRKGINWSUIPIZ6ZBCTV6N3KSHES/>
- MISC - <https://www.drupal.org/sa-contrib-2022-004>
- MISC - <https://www.oracle.com/security-alerts/cpuapr2022.html>
- MLIST - [\[debian-lts-announce\] 20220119 \[SECURITY\] \[DLA-2889-1\] drupal7 security update](#)
- N/A - N/A
- info - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-41182>

## Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 7.0; versions up to (excluding) 7.86
- cpe:2.3:a:jqueryui:jquery\_ui:\*:\*:\*:\*:\* versions up to (excluding) 1.13.0
- cpe:2.3:a:oracle:agile\_plm:9.3.6:\*:\*:\*:\*
- cpe:2.3:a:oracle:application\_express:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:banking\_platform:2.9.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:banking\_platform:2.12.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:\*:\*:\*:\*:\* versions up to (excluding) 23.1
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:23.1:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_interactive\_session\_recorder:6.4:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.3:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.4:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:5.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_inventory\_management:9.1.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_materials\_control:18.1:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_suite8:\*:\*:\*:\*:\* versions from (including) 8.11.0; versions up to (including) 8.14.0
- cpe:2.3:a:oracle:hospitality\_suite8:8.10.2:\*:\*:\*:\*
- cpe:2.3:a:oracle:jd\_edwards\_enterpriseone\_tools:\*:\*:\*:\*:\* versions up to (including) 9.2.6.3
- cpe:2.3:a:oracle:mysql\_enterprise\_monitor:\*:\*:\*:\*:\* versions up to (including) 8.0.29
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.58:\*:\*:\*:\*
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.59:\*:\*:\*:\*
- cpe:2.3:a:oracle:policy\_automation:\*:\*:\*:\*:\* versions from (including) 12.2.0; versions up to (including) 12.2.25
- cpe:2.3:a:oracle:primavera\_unifier:\*:\*:\*:\*:\* versions from (including) 17.7; versions up to (including) 17.12
- cpe:2.3:a:oracle:primavera\_unifier:17.7:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.8:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.9:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.10:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.11:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.12:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:18.8:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:19.12:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:20.12:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:21.12:\*:\*:\*:\*

- cpe:2.3:a:oracle:rest\_data\_services:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:rest\_data\_services:22.1.1:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.3.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.4.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:14.1.1.0.0:\*:\*:\*:\*
- cpe:2.3:a:tenable:tenable.sc:\*:\*:\*:\*:\* versions up to (excluding) 5.21.0

## **CVE-2021-41183** suppressed

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `\*Text` options of the DatePicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `\*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `\*Text` options from untrusted sources.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: JavaDoc embedded JQuery UI - requires updated Java Version with newer javadoc

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:

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

References:

- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20211118-0004/>
- CONFIRM - <https://www.drupal.org/sa-core-2022-001>
- CONFIRM - <https://www.drupal.org/sa-core-2022-002>
- CONFIRM - <https://www.tenable.com/security/tns-2022-09>
- MISC - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
- MISC - <https://bugs.jqueryui.com/ticket/15284>
- MISC - <https://github.com/jquery/jquery-ui/pull/1953>
- MISC - <https://lists.debian.org/debian-lts-announce/2023/08/msg00040.html>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/HVKIOWSXL2RF2ULNAP7PHESYCF5ZIJJE3/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/NXIUUBRVLA4E7G7MMIKCEN75YN7UFERW/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/O74SXY7RGXREQDQUDQD4BPJ4QQTD2XQ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SGSY236PYSFYIEBRGDERLA7OSY6D7XL4/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SNXA7XRKGINWSUIPIZ6BCTV6N3KSHES/>
- MISC - <https://www.drupal.org/sa-contrib-2022-004>
- MISC - <https://www.oracle.com/security-alerts/cpuapr2022.html>
- MLIST - [\[debian-lts-announce\] 20220119 \[SECURITY\] \[DLA-2889-1\] drupal7 security update](#)
- N/A - [N/A](#)
- info - <https://bugs.jqueryui.com/ticket/15284>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-41183>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 7.0; versions up to (excluding) 7.86
- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 9.2.0; versions up to (excluding) 9.2.11
- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 9.3.0; versions up to (excluding) 9.3.3
- cpe:2.3:a:jqueryui:jquery\_ui:\*:\*:\*:\*:\* versions up to (excluding) 1.13.0
- cpe:2.3:a:oracle:agile\_plm:9.3.6:\*:\*:\*:\*
- cpe:2.3:a:oracle:application\_express:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:banking\_platform:2.9.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:banking\_platform:2.12.0:\*:\*:\*:\*



- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:\*:\*:\*:\*:\* versions up to (excluding) 23.1
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:23.1:\*:\*:\*:\*:
- cpe:2.3:a:oracle:communications\_interactive\_session\_recorder:6.4:\*:\*:\*:\*:
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.3:\*:\*:\*:\*:
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.4:\*:\*:\*:\*:
- cpe:2.3:a:oracle:communications\_operations\_monitor:5.0:\*:\*:\*:\*:
- cpe:2.3:a:oracle:hospitality\_inventory\_management:9.1.0:\*:\*:\*:\*:
- cpe:2.3:a:oracle:hospitality\_suite8:\*:\*:\*:\*:\* versions from (including) 8.11.0; versions up to (including) 11.14.0
- cpe:2.3:a:oracle:hospitality\_suite8:8.10.2:\*:\*:\*:\*:
- cpe:2.3:a:oracle:jd\_edwards\_enterpriseone\_tools:\*:\*:\*:\*:\* versions up to (including) 9.2.6.3
- cpe:2.3:a:oracle:mysql\_enterprise\_monitor:\*:\*:\*:\*:\* versions up to (including) 8.0.29
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.58:\*:\*:\*:\*:
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.59:\*:\*:\*:\*:
- cpe:2.3:a:oracle:policy\_automation:\*:\*:\*:\*:\* versions from (including) 12.2.0; versions up to (including) 12.2.5
- cpe:2.3:a:oracle:primavera\_gateway:\*:\*:\*:\*:\* versions from (including) 17.7; versions up to (including) 17.12
- cpe:2.3:a:oracle:primavera\_gateway:18.8.0:\*:\*:\*:\*:
- cpe:2.3:a:oracle:primavera\_gateway:19.12.0:\*:\*:\*:\*:
- cpe:2.3:a:oracle:primavera\_gateway:20.12.0:\*:\*:\*:\*:
- cpe:2.3:a:oracle:primavera\_gateway:21.12.0:\*:\*:\*:\*:
- cpe:2.3:a:oracle:rest\_data\_services:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:rest\_data\_services:22.1.1:\*:\*:\*:\*:
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.3.0:\*:\*:\*:\*:
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.4.0:\*:\*:\*:\*:
- cpe:2.3:a:oracle:weblogic\_server:14.1.1.0.0:\*:\*:\*:\*:
- cpe:2.3:a:tenable:tenable.sc:\*:\*:\*:\*:\* versions up to (excluding) 5.21.0

#### **CVE-2021-41184** suppressed

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: JavaDoc embedded JQuery UI - requires updated Java Version with newer javadoc

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:

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

References:

- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20211118-0004/>
- CONFIRM - <https://www.drupal.org/sa-core-2022-001>
- CONFIRM - <https://www.tenable.com/security/tns-2022-09>
- MISC - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
- MISC - <https://github.com/jquery/jquery-ui/commit/effa323f1505f2ce7a324e4f429fa9032c72f280>
- MISC - <https://lists.debian.org/debian-its-announce/2023/08/msg00040.html>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/HVKIOWSXL2RF2ULNAP7PHESYCF5ZIE3/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/NXIUUBRVLA4E7G7MMIKCEN75YN7UFERW/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/O74SXYY7RGXREQDQUDQD4BPJ4QQTD2XQ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SGSY236PYSFYIEBRGDERLA7OSY6D7XL4/>



- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SNXA7XRKGINWSUIPIZ6ZBCTV6N3KSHES/>
- MISC - <https://www.oracle.com/security-alerts/cpuapr2022.html>
- N/A - [N/A](#)
- info - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-41184>

#### Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 7.0; versions up to (excluding) 7.86
- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 9.2.0; versions up to (excluding) 9.2.11
- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 9.3.0; versions up to (excluding) 9.3.3
- cpe:2.3:a:jqueryui:jquery\_ui:\*:\*:\*:\*:\* versions up to (excluding) 1.13.0
- cpe:2.3:a:oracle:agile\_plm:9.3.6:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:application\_express:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:banking\_platform:2.9.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:banking\_platform:2.12.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:\*:\*:\*:\*:\* versions up to (excluding) 23.1
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:23.1:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_interactive\_session\_recorder:6.4:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.3:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.4:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:5.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_inventory\_management:9.1.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_materials\_control:18.1:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_suite8:\*:\*:\*:\*:\* versions from (including) 8.11.0; versions up to (including) 8.14.0
- cpe:2.3:a:oracle:hospitality\_suite8:8.10.2:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:jd\_edwards\_enterpriseone\_tools:\*:\*:\*:\*:\* versions up to (including) 9.2.6.3
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.58:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.59:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:policy\_automation:\*:\*:\*:\*:\* versions from (including) 12.2.0; versions up to (including) 12.2.25
- cpe:2.3:a:oracle:primavera\_unifier:\*:\*:\*:\*:\* versions from (including) 17.7; versions up to (including) 17.12
- cpe:2.3:a:oracle:primavera\_unifier:18.8:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:19.12:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:20.12:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:21.12:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:rest\_data\_services:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:rest\_data\_services:22.1.1:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.3.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.4.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:14.1.1.0.0:\*:\*:\*:\*:\*
- cpe:2.3:a:tenable:tenable.sc:\*:\*:\*:\*:\* versions up to (excluding) 5.21.0

#### **CVE-2022-31160** suppressed

jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-site scripting. Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. Calling `.checkboxradio("refresh")` on such a widget and the initial HTML contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery UI 1.13.2. To remediate the issue, someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: JavaDoc embedded JQuery UI - requires updated Java Version with newer javadoc

CVSSv3:

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

#### References:

- - [FEDORA-2022-1a01ed37e2](#)
- - [FEDORA-2022-22d8ba36d0](#)
- - [FEDORA-2022-7291b78111](#)
- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-h6gj-6jjq-h8g9>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220909-0007/>
- MISC - <https://blog.jqueryui.com/2022/07/jquery-ui-1-13-2-released/>
- MISC - <https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fc96bf5862c5646c787020ba3f9>
- MISC - <https://www.drupal.org/sa-contrib-2022-052>
- MLIST - [\[debian-lts-announce\] 20221207 \[SECURITY\] \[DLA 3230-1\] jqueryui security update](#)
- info - <https://github.com/advisories/GHSA-h6gj-6jjq-h8g9>
- info - <https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fc96bf5862c5646c787020ba3f9>
- info - <https://github.com/jquery/jquery-ui/issues/2101>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2022-31160>

#### Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:jquery\_ui\_checkboxradio:8.x-1.0:\*:\*:\*:\*:drupal:\*:\*
- cpe:2.3:a:drupal:jquery\_ui\_checkboxradio:8.x-1.1:\*:\*:\*:\*:drupal:\*:\*
- cpe:2.3:a:drupal:jquery\_ui\_checkboxradio:8.x-1.2:\*:\*:\*:\*:drupal:\*:\*
- cpe:2.3:a:drupal:jquery\_ui\_checkboxradio:8.x-1.3:\*:\*:\*:\*:drupal:\*:\*
- cpe:2.3:a:jqueryui:jquery\_ui:\*:\*:\*:\*:jquery:\*:\* versions up to (excluding) 1.13.2
- cpe:2.3:a:netapp:oncommand\_insight:\*:\*:\*:\*:\*:netapp:\*:\*

### reporting.zip: reporting-javadoc.jar: jquery-ui.min.js

**File Path:** /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/designer/build/tmp/dependencies/i-net Clear Reports Designer/plugins/reporting.zip/reporting-javadoc.jar/jquery/jquery-ui.min.js

**MD5:** 28d157e58272e91b054c254eab737df0

**SHA1:** 4165e40107b31b0ce5f022f579635fccb887bef9

**SHA256:** 76e849220d7fe7778affeaaaf0806e48bbb69a5ec5b8c8b8f5f3cd89439a6dedc

#### Evidence



#### Related Dependencies



#### Suppressed Identifiers

- None

#### Suppressed Vulnerabilities



[CVE-2021-41182](#) suppressed

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is

now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

## CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: JavaDoc embedded JQuery UI - requires updated Java Version with newer javadoc

### CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

### CVSSv3:

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

### References:

- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20211118-0004/>
- CONFIRM - <https://www.drupal.org/sa-core-2022-002>
- CONFIRM - <https://www.tenable.com/security/tns-2022-09>
- MISC - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
- MISC - <https://github.com/jquery/jquery-ui/pull/1954/commits/6809ce843e5ac4128108ea4c15cbc100653c2b63>
- MISC - <https://lists.debian.org/debian-lts-announce/2023/08/msg00040.html>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/HVKIOWSXL2RF2ULNAP7PHESYCFJSZIE3/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/NXIUUBRVLA4E7G7MMIKCEN75YN7UFERW/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/O74SXYY7RGXREQDQUDQD4BPJ4QQTD2XQ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SGSY236PYSFYIEBRGDERLA7OSY6D7XL4/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SNXA7XRKGINWSUIPIZ6ZBCTV6N3KSHES/>
- MISC - <https://www.drupal.org/sa-contrib-2022-004>
- MISC - <https://www.oracle.com/security-alerts/cpuapr2022.html>
- MLIST - [\[debian-lts-announce\] 20220119 \[SECURITY\] \[DLA-2889-1\] drupal7 security update](#)
- N/A - [N/A](#)
- info - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-41182>

### Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 7.0; versions up to (excluding) 7.86
- cpe:2.3:a:jqueryui:jquery\_ui:\*:\*:\*:\*:\* versions up to (excluding) 1.13.0
- cpe:2.3:a:oracle:agile\_plm:9.3.6:\*:\*:\*:\*
- cpe:2.3:a:oracle:application\_express:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:banking\_platform:2.9.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:banking\_platform:2.12.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:\*:\*:\*:\*:\* versions up to (excluding) 23.1
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:23.1:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_interactive\_session\_recorder:6.4:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.3:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.4:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:5.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_inventory\_management:9.1.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_materials\_control:18.1:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_suite8:\*:\*:\*:\*:\* versions from (including) 8.11.0; versions up to (including) 8.14.0
- cpe:2.3:a:oracle:hospitality\_suite8:8.10.2:\*:\*:\*:\*
- cpe:2.3:a:oracle:jd\_edwards\_enterpriseone\_tools:\*:\*:\*:\*:\* versions up to (including) 9.2.6.3
- cpe:2.3:a:oracle:mysql\_enterprise\_monitor:\*:\*:\*:\*:\* versions up to (including) 8.0.29
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.58:\*:\*:\*:\*
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.59:\*:\*:\*:\*

- cpe:2.3:a:oracle:policy\_automation:\*:\*:\*:\*:\* versions from (including) 12.2.0; versions up to (including) 12.2.25
- cpe:2.3:a:oracle:primavera\_unifier:\*:\*:\*:\*:\* versions from (including) 17.7; versions up to (including) 17.12
- cpe:2.3:a:oracle:primavera\_unifier:17.7:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.8:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.9:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.10:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.11:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:17.12:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:18.8:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:19.12:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:20.12:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:21.12:\*:\*:\*:\*
- cpe:2.3:a:oracle:rest\_data\_services:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:rest\_data\_services:22.1.1:\*:\*:\*:
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.3.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.4.0:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:14.1.1.0.0:\*:\*:\*:\*
- cpe:2.3:a:tenable:tenable.sc:\*:\*:\*:\*:\* versions up to (excluding) 5.21.0

### **CVE-2021-41183** suppressed

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `\*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `\*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `\*Text` options from untrusted sources.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: JavaDoc embedded JQuery UI - requires updated Java Version with newer javadoc

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:

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

References:

- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgf6-hvh4>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20211118-0004/>
- CONFIRM - <https://www.drupal.org/sa-core-2022-001>
- CONFIRM - <https://www.drupal.org/sa-core-2022-002>
- CONFIRM - <https://www.tenable.com/security/tns-2022-09>
- MISC - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
- MISC - <https://bugs.jqueryui.com/ticket/15284>
- MISC - <https://github.com/jquery/jquery-ui/pull/1953>
- MISC - <https://lists.debian.org/debian-lts-announce/2023/08/msg00040.html>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/HVKIOWSXL2RF2ULNAP7PHESYCF5ZIJJE3/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/NXIUUBRVLA4E7G7MMIKCEN75YN7UFERW/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/O74SXY7RGXREQDQUDQD4BPJ4QQTD2XQ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SGSY236PYSFYIEBRGDERLA7OSY6D7XL4/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SNXA7XRKGINWSUIPIZ6ZBCTV6N3KSHES/>
- MISC - <https://www.drupal.org/sa-contrib-2022-004>
- MISC - <https://www.oracle.com/security-alerts/cpuapr2022.html>
- MLIST - [\[debian-lts-announce\] 20220119 \[SECURITY\] \[DLA-2889-1\] drupal7 security update](#)
- N/A - [N/A](#)
- info - <https://bugs.jqueryui.com/ticket/15284>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-41183>

## Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 7.0; versions up to (excluding) 7.86
- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 9.2.0; versions up to (excluding) 9.2.11
- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 9.3.0; versions up to (excluding) 9.3.3
- cpe:2.3:a:jqueryui:jquery\_ui:\*:\*:\*:\*:\* versions up to (excluding) 1.13.0
- cpe:2.3:a:oracle:agile\_plm:9.3.6:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:application\_express:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:banking\_platform:2.9.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:banking\_platform:2.12.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:\*:\*:\*:\*:\* versions up to (excluding) 23.1
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:23.1:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_interactive\_session\_recorder:6.4:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.3:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.4:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:5.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_inventory\_management:9.1.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_suite8:\*:\*:\*:\*:\* versions from (including) 8.11.0; versions up to (including) 11.14.0
- cpe:2.3:a:oracle:hospitality\_suite8:8.10.2:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:jd\_edwards\_enterpriseone\_tools:\*:\*:\*:\*:\* versions up to (including) 9.2.6.3
- cpe:2.3:a:oracle:mysql\_enterprise\_monitor:\*:\*:\*:\*:\* versions up to (including) 8.0.29
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.58:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.59:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:policy\_automation:\*:\*:\*:\*:\* versions from (including) 12.2.0; versions up to (including) 12.2.5
- cpe:2.3:a:oracle:primavera\_gateway:\*:\*:\*:\*:\* versions from (including) 17.7; versions up to (including) 17.12
- cpe:2.3:a:oracle:primavera\_gateway:18.8.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_gateway:19.12.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_gateway:20.12.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_gateway:21.12.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:rest\_data\_services:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:rest\_data\_services:22.1.1:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.3.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.4.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:14.1.1.0.0:\*:\*:\*:\*:\*
- cpe:2.3:a:tenable:tenable.sc:\*:\*:\*:\*:\* versions up to (excluding) 5.21.0

## **CVE-2021-41184** suppressed

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: JavaDoc embedded JQuery UI - requires updated Java Version with newer javadoc

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:

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

References:

- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20211118-0004/>
- CONFIRM - <https://www.drupal.org/sa-core-2022-001>



- CONFIRM - <https://www.tenable.com/security/tns-2022-09>
- MISC - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
- MISC - <https://github.com/jquery/jquery-ui/commit/effa323f1505f2ce7a324e4f429fa9032c72f280>
- MISC - <https://lists.debian.org/debian-lts-announce/2023/08/msg00040.html>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/HVKIOWSXL2RF2ULNAP7PHESYCF5ZIJIE3/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/NXIUUBRVLA4E7G7MMIKCEN75YN7UFERW/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/O74SXY7RGXREQDQUDQD4BPJ4QQTD2XQ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SGSY236PYSFYIEBRGDERLA7OSY6D7XL4/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SNXA7XRKGINWSUIPIZ6ZBCTV6N3KSHES/>
- MISC - <https://www.oracle.com/security-alerts/cpuapr2022.html>
- N/A - N/A
- info - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-41184>

#### Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 7.0; versions up to (excluding) 7.86
- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 9.2.0; versions up to (excluding) 9.2.11
- cpe:2.3:a:drupal:drupal:\*:\*:\*:\*:\* versions from (including) 9.3.0; versions up to (excluding) 9.3.3
- cpe:2.3:a:jqueryui:jquery\_ui:\*:\*:\*:\*:\* versions up to (excluding) 1.13.0
- cpe:2.3:a:oracle:agile\_plm:9.3.6:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:application\_express:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:banking\_platform:2.9.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:banking\_platform:2.12.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:\*:\*:\*:\*:\* versions up to (excluding) 23.1
- cpe:2.3:a:oracle:big\_data\_spatial\_and\_graph:23.1:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_interactive\_session\_recorder:6.4:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.3:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:4.4:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:communications\_operations\_monitor:5.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_inventory\_management:9.1.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_materials\_control:18.1:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:hospitality\_suite8:\*:\*:\*:\*:\* versions from (including) 8.11.0; versions up to (including) 8.14.0
- cpe:2.3:a:oracle:hospitality\_suite8:8.10.2:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:jd\_edwards\_enterpriseone\_tools:\*:\*:\*:\*:\* versions up to (including) 9.2.6.3
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.58:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.59:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:policy\_automation:\*:\*:\*:\*:\* versions from (including) 12.2.0; versions up to (including) 12.2.25
- cpe:2.3:a:oracle:primavera\_unifier:\*:\*:\*:\*:\* versions from (including) 17.7; versions up to (including) 17.12
- cpe:2.3:a:oracle:primavera\_unifier:18.8:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:19.12:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:20.12:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:primavera\_unifier:21.12:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:rest\_data\_services:\*:\*:\*:\*:\* versions up to (excluding) 22.1.1
- cpe:2.3:a:oracle:rest\_data\_services:22.1.1:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.3.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:12.2.1.4.0:\*:\*:\*:\*:\*
- cpe:2.3:a:oracle:weblogic\_server:14.1.1.0.0:\*:\*:\*:\*:\*
- cpe:2.3:a:tenable:tenable.sc:\*:\*:\*:\*:\* versions up to (excluding) 5.21.0

**CVE-2022-31160** suppressed

jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-site scripting. Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents

considered as the input label. Calling `.checkboxradio("refresh")` on such a widget and the initial HTML contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery UI 1.13.2. To remediate the issue, someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Notes: JavaDoc embedded JQuery UI - requires updated Java Version with newer javadoc

CVSSv3:

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

References:

- - [FEDORA-2022-1a01ed37e2](#)
- - [FEDORA-2022-22d8ba36d0](#)
- - [FEDORA-2022-7291b78111](#)
- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-h6gj-6jjq-h8g9>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220909-0007/>
- MISC - <https://blog.jqueryui.com/2022/07/jquery-ui-1-13-2-released/>
- MISC - <https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fc96bf5862c5646c787020ba3f9>
- MISC - <https://www.drupal.org/sa-contrib-2022-052>
- MLIST - [\[debian-lts-announce\] 20221207 \[SECURITY\] \[DLA 3230-1\] jqueryui security update](#)
- info - <https://github.com/advisories/GHSA-h6gj-6jjq-h8g9>
- info - <https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fc96bf5862c5646c787020ba3f9>
- info - <https://github.com/jquery/jquery-ui/issues/2101>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2022-31160>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:jquery\_ui\_checkboxradio:8.x-1.0:\*:\*:\*:\*:drupal:\*:\*
- cpe:2.3:a:drupal:jquery\_ui\_checkboxradio:8.x-1.1:\*:\*:\*:\*:drupal:\*:\*
- cpe:2.3:a:drupal:jquery\_ui\_checkboxradio:8.x-1.2:\*:\*:\*:\*:drupal:\*:\*
- cpe:2.3:a:drupal:jquery\_ui\_checkboxradio:8.x-1.3:\*:\*:\*:\*:drupal:\*:\*
- cpe:2.3:a:jqueryui:jquery\_ui:\*:\*:\*:\*:jquery:\*:\* versions up to (excluding) 1.13.2
- cpe:2.3:a:netapp:oncommand\_insight:\*:\*:\*:\*:\*

## reporting.zip: reporting-javadoc.jar: jszip.js

**File Path:** /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/designer/build/tmp/dependencies/i-net Clear Reports Designer/plugins/reporting.zip/reporting-javadoc.jar/jquery/jszip/dist/jszip.js

**MD5:** 445655f2b60614c242f0c073c319ebd3

**SHA1:** 2f46d4b06054852cdde51cee3764f71b8658da87

**SHA256:** 6c18a4b2cee69dd705e8a9ac911e2284f4a5c68c86031b86e067ffaf3a253938

Evidence



Related Dependencies



Suppressed Identifiers



- None

## Suppressed Vulnerabilities



### [CVE-2022-48285](#) suppressed

loadAsync in JSZip before 3.8.0 allows Directory Traversal via a crafted ZIP archive.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Notes: JavaDoc embedded library. file name: reporting-22.10.zip: reporting-javadoc.jar: jszip.js

CVSSv3:

- HIGH (7.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

References:

- MISC - <https://exchange.xforce.ibmcloud.com/vulnerabilities/244499>
- MISC - <https://github.com/Stuk/jszip/commit/2edab366119c9ee948357c02f1206c28566cdf15>
- MISC - <https://github.com/Stuk/jszip/compare/v3.7.1...v3.8.0>
- MISC - <https://www.mend.io/vulnerability-database/WS-2023-0004>
- info - <https://stuk.github.io/jszip/CHANGES.html>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:jszip\_project:jszip:\*:\*:\*:\*:node.js:\*:\* versions up to (excluding) 3.8.0

### [CVE-2021-23413](#) suppressed

This affects the package jszip before 3.7.0. Crafting a new zip file with filenames set to Object prototype values (e.g \_\_proto\_\_, toString, etc) results in a returned object with a modified prototype instance.

NVD-CWE-noinfo

Notes: JavaDoc embedded library. file name: reporting-22.10.zip: reporting-javadoc.jar: jszip.js

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:

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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-jg8v-48h5-wgxg>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-23413>
- info - <https://security.snyk.io/vuln/SNYK-JS-JSZIP-1251497>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:jszip\_project:jszip:\*:\*:\*:\*:node.js:\*:\* versions up to (excluding) 3.7.0

## reporting.zip: reporting-javadoc.jar: jszip.min.js

**File Path:** /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/designer/build/tmp/dependencies/i-net Clear Reports Designer/plugins/reporting.zip/reporting-javadoc.jar/jquery/jszip/dist/jszip.min.js

**MD5:** dc5d2aac976b1ad09faa452b4ce37519

**SHA1:** 3437dfa4dce6aa98c78ff6768de5694a70768892

**SHA256:** 832e56e7fad75a5b965c546f31614531586871fa417bb4dfe125b658c7e3b381

### Evidence



### Related Dependencies



### Suppressed Identifiers

- None

### Suppressed Vulnerabilities



#### [CVE-2022-48285](#) suppressed

loadAsync in JSZip before 3.8.0 allows Directory Traversal via a crafted ZIP archive.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Notes: JavaDoc embedded library. file name: reporting-22.10.zip: reporting-javadoc.jar: jszip.js

CVSSv3:

- HIGH (7.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

References:

- MISC - <https://exchange.xforce.ibmcloud.com/vulnerabilities/244499>
- MISC - <https://github.com/Stuk/jszip/commit/2edab366119c9ee948357c02f1206c28566cdf15>
- MISC - <https://github.com/Stuk/jszip/compare/v3.7.1...v3.8.0>
- MISC - <https://www.mend.io/vulnerability-database/WS-2023-0004>
- info - <https://stuk.github.io/jszip/CHANGES.html>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:jszip\_project:jszip:\*:\*:\*:\*:node.js:\* versions up to (excluding) 3.8.0

#### [CVE-2021-23413](#) suppressed

This affects the package jszip before 3.7.0. Crafting a new zip file with filenames set to Object prototype values (e.g. \_\_proto\_\_, toString, etc) results in a returned object with a modified prototype instance.

NVD-CWE-noinfo

Notes: JavaDoc embedded library. file name: reporting-22.10.zip: reporting-javadoc.jar: jszip.js

CVSSv2:

- Base Score: MEDIUM (5.0)

- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:

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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-jg8v-48h5-wgxg>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-23413>
- info - <https://security.snyk.io/vuln/SNYK-JS-JSZIP-1251497>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:jszip\_project:jszip:\*:\*:\*:\*:\*:node.js:\*:\* versions up to (excluding) 3.7.0

This report contains data retrieved from the [National Vulnerability Database](#).

This report may contain data retrieved from the [NPM Public Advisories](#).

This report may contain data retrieved from [RetireJS](#).

This report may contain data retrieved from the [Sonatype OSS Index](#).