



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-installer'

clear-reports:designer-installer:24.10

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

- *dependency-check version:* 10.0.3
- *Report Generated On:* Thu, 19 Sep 2024 18:50:54 +0200
- *Dependencies Scanned:* 217 (201 unique)
- *Vulnerable Dependencies:* 0
- *Vulnerabilities Found:* 0
- *Vulnerabilities Suppressed:* 2 ([show](#))
- ...

## Summary

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

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

## Dependencies (vulnerable)

## Suppressed Vulnerabilities



decoder.svg.zip: xmlgraphics-commons.jar

**File Path:** /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/designer/build/tmp/dependencies/i-net Clear Reports Designer/plugins/decoder.svg.zip/xmlgraphics-commons.jar

**MD5:** ec712218e2391e64672fd8ed1e9e1d71

**SHA1:** 336ddd6d0a244cdeb26a298fb7c3a5fd45449db

**SHA256:** 1fe37a1927bdd699730f0ad39f50a699c9ab4dff0ad047dff1e846cb120ae2b1

**Referenced In Project/Scope:** designer-installer

Evidence



Suppressed Identifiers

- `cpe:2.3:a:apache:commons_net:2.7:*:*:*:*:*` suppressed (*Confidence:Low*)
  - Notes: XML Graphics Common has a false positive match on Apache Commons Net

### Suppressed Vulnerabilities

#### [CVE-2021-37533](#) suppressed

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>.

CWE-20 Improper Input Validation

CVSSv3:

- MEDIUM (6.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:2.8/RC:R/MAV:A

References:

- [security@apache.org](mailto:security@apache.org) - [ISSUE\\_TRACKING,MAILING\\_LIST,THIRD\\_PARTY\\_ADVISORY](#)
- [security@apache.org](mailto:security@apache.org) - [ISSUE\\_TRACKING,MAILING\\_LIST,VENDOR\\_ADVISORY](#)
- [security@apache.org](mailto:security@apache.org) - [MAILING\\_LIST,THIRD\\_PARTY\\_ADVISORY](#)
- [security@apache.org](mailto:security@apache.org) - [THIRD\\_PARTY\\_ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:apache:commons\\_net:\\*:\\*:\\*:\\*:\\* versions up to \(excluding\) 3.9.0](#)

## 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/script-dir/jquery-ui.min.js

**MD5:** 32059df39c14a910ccc2325f6a3cd62f

**SHA1:** d3289f1b527a3f054d303ec769402e037fbfcf4b

**SHA256:** 672f278182cdf04f3c62a5b8d93f406791854a28791f27aecdb9981573c61424

**Referenced In Project/Scope:** designer-installer

#### Evidence

#### Related Dependencies

#### Suppressed Identifiers

- None

**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/E:2.8/RC:R/MAV:A

References:

- 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>
- security-advisories@github.com - [EXPLOIT,MITIGATION,RELEASE\\_NOTES,THIRD\\_PARTY\\_ADVISORY](#)
- security-advisories@github.com - [MAILING\\_LIST,THIRD\\_PARTY\\_ADVISORY](#)
- security-advisories@github.com - [PATCH,THIRD\\_PARTY\\_ADVISORY](#)
- security-advisories@github.com - [RELEASE\\_NOTES,VENDOR\\_ADVISORY](#)
- security-advisories@github.com - [THIRD\\_PARTY\\_ADVISORY](#)
- security-advisories@github.com - [THIRD\\_PARTY\\_ADVISORY](#)

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:-:\*:\*:\*:\*:\*

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

This report may contain data retrieved from the [CISA Known Exploited Vulnerability Catalog](#).

This report may contain data retrieved from the [Github Advisory Database \(via NPM Audit API\)](#).

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

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