



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 ':server'

helpdesk:server:23.10

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

- *dependency-check version:* 7.4.4
- *Report Generated On:* Thu, 23 Nov 2023 13:43:22 +0100
- *Dependencies Scanned:* 3051 (2142 unique)
- *Vulnerable Dependencies:* 0
- *Vulnerabilities Found:* 0
- *Vulnerabilities Suppressed:* 21
- ...

## Summary

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

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

## Dependencies

## Suppressed Vulnerabilities



cowork.zip: cowork-javadoc.jar: jquery-ui.js

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/cowork.zip/cowork-javadoc.jar/jquery/jquery-ui.js

**MD5:** 3e34f50eab2e13d720c93e44ac5cb7ca

**SHA1:** c432ac324c727a86a9a54eff1b90d79e115e3f16

**SHA256:** 712e2e2efe1717a1e10aee0e02163e1deadf88760ade58b5cdf333ea6de5247

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/HVKIOWSXL2RF2ULNAP7PHESYCFSZIJ3/>
- 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/HVKIOWSXL2RF2ULNAP7PHESYCFSTZJE3/>
- 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/HVKIOWSXL2RF2ULNAP7PHESYCFSTZIE3/>
- 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/O74SXY7RGXREQDQDQD4BPJ4QQTD2XQ/>
- 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:\*:\*:\*:\*:\*



**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/cowork.zip/cowork-javadoc.jar/jquery/jquery-ui.min.js  
**MD5:** 28d157e58272e91b054c254eab737df0  
**SHA1:** 4165e40107b31b0ce5f022f579635fccb887bef9  
**SHA256:** 76e849220d7fe7778affeaa0806e48bbb69a5ec5b8c8b8f5f3cd89439a6dedc

#### 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/HVKIOWSXL2RF2ULNAP7PHESYCFSZIJ3/>
- 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/SNXA7XRKGINWSUIPIZ6ZBCTV6N3KSHE/>
- 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-2021-41182](#) 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-pg6f-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/HVKIOWSXL2RF2ULNAP7PHESYCF5ZIJ3/>
- 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/HVKIOWSXL2RF2ULNAP7PHESYCF5ZIJ3/>
- 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:\*\*\*\*\*jquery:.\* 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/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9>
- 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/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9>
- 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:\*:\*:\*:\*:\*:

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

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/cowork.zip/cowork-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

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

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/cowork.zip/cowork-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

## remotegui.zip: echo2extras-app.jar

### Description:

Echo2 Extras

### License:



MPL 1.1: <http://www.mozilla.org/MPL/MPL-1.1.html>  
LGPL 2.1: <http://www.gnu.org/licenses/lgpl-2.1.html>  
GPL 2.0: <http://www.gnu.org/licenses/gpl-2.0.html>

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems  
/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/remotegui.zip  
/echo2extras-app.jar

**MD5:** e1ba37ba20c3021c38e362cac081d986

**SHA1:** 64e7748149ca2af54ee693c8e232343d64c1b966

**SHA256:** ad4489475b3c77aeeb62ec1c1bc211c8659b84649fdb1e72f4ee6e005b21e37b

#### Evidence



#### Related Dependencies



#### Suppressed Identifiers

- None

#### Suppressed Vulnerabilities



##### [CVE-2009-5135](#) suppressed

The Java XML parser in Echo before 2.1.1 and 3.x before 3.0.b6 allows remote attackers to read arbitrary files via a request containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

CWE-20 Improper Input Validation

Notes: Ignore echo2 apps, because we are using v2.1.1 which is the latest applicable. But the official libs do not have version number.

CVSSv2:

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

References:

- BUGTRAQ - [20090310 SEC Consult SA-20090305-0 :: NextApp Echo XML Injection Vulnerability](#)
- CONFIRM - <http://echo.nextapp.com/site/node/5742>
- EXPLOIT-DB - [8191](#)
- MISC - [https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories\\_txt/20090305-0\\_echo\\_nextapp\\_xml\\_injection.txt](https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20090305-0_echo_nextapp_xml_injection.txt)
- SECUNIA - [34218](#)
- VUPEN - [ADV-2009-0653](#)
- XF - [echo2-xml-information-disclosure\(49167\)](#)

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

- [cpe:2.3:a:nextapp:echo:2.1.0:beta4:.\\*.\\*.\\*.\\*.\\*](#)
- ...

**Description:**

WebJar for jQuery

**License:**

MIT License: <https://github.com/jquery/jquery/blob/master/MIT-LICENSE.txt>

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/remotegui.zip/jquery.jar

**MD5:** 4af65e569248d8a2411f66498d720280

**SHA1:** c3dc40b1b5f24c56afa36fd9a463bb9f378ac4ab

**SHA256:** de28c4da0ea9f16101352dd3582ec8021ee5e2de5f45104ca171876003d54db6

**Evidence**



**Suppressed Identifiers**

- None

**Suppressed Vulnerabilities**



**CVE-2019-11358** (OSSINDEX) suppressed

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable \_\_proto\_\_ property, it could extend the native Object.prototype.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2019-11358> for details

CWE-1321

Notes: file name: remotegui.jar: jquery.min.js - We can not yet upgrade to a newer version due to dependencies. We do, however, not directly use the functionality that is being CVEd

CVSSv2:

- Base Score: MEDIUM (6.1)
- Vector: /AV:N/AC:L/Au:C/L/I:L/A:N

References:

- OSSINDEX - [\[CVE-2019-11358\] CWE-1321](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11358>
- OSSIndex - <https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/>
- OSSIndex - <https://github.com/cbeust/testng/issues/2150>
- OSSIndex - <https://github.com/jquery/jquery/pull/4333>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.webjars:jquery:2.2.4:\*:\*:\*:\*:\*

**CVE-2020-11023** (OSSINDEX) suppressed

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

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

Notes: file name: remotegui.jar: jquery.min.js - We can not yet upgrade to a newer version due to dependencies. We do, however, not directly use the functionality that is being CVEd

CVSSv2:

- Base Score: MEDIUM (6.1)
- Vector: /AV:N/AC:L/Au:C/L/I:L/A:N

References:

- OSSINDEX - [\[CVE-2020-11023\] CWE-79: Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11023>
- OSSIndex - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>
- OSSIndex - <https://jquery.com/upgrade-guide/3.5/>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.webjars:jquery:2.2.4:\*:\*:\*:\*:\*

## repository.zip: milton-api.jar

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems /HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/repository.zip/milton-api.jar

**MD5:** 35d4685b67d7ba1b0271f8289e0c330b

**SHA1:** 1a76399457cf546d6b57bd329c2fc081edaafb11

**SHA256:** e2801623bbb552404a132abcddf5ee13fc49b095ae4d00cb305d363b0240d2dc

### Evidence



### Related Dependencies



### Suppressed Identifiers

- None

### Suppressed Vulnerabilities



[CVE-2015-7326](#) suppressed

XML External Entity (XXE) vulnerability in Milton Webdav before 2.7.0.3.

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

Notes: The Milton library is being used for WebDav from the Repository Browser. It is way older

than the one with the issue, but should be removed timely.

#### CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

#### CVSSv3:

- CRITICAL (9.8)
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

#### References:

- BID - [77392](#)
- BUGTRAQ - [20151102 CVE-2015-7326 \(XXE vulnerability in Milton Webdav\)](#)
- CONFIRM - <https://github.com/miltonio/milton2/commit/5f81b0c48a817d4337d8b0e99ea0b4744ecd720b>
- CONFIRM - <https://github.com/miltonio/milton2/commit/b41072b>
- CONFIRM - <https://github.com/miltonio/milton2/commit/b5851c1>
- MISC - <http://packetstormsecurity.com/files/134178/Milton-Webdav-2.7.0.1-XXE-Injection.html>

#### Vulnerable Software & Versions:

- [cpe:2.3:a:milton:webdav:\\*:\\*:\\*:\\*:\\* versions up to \(including\) 2.7.0.1](#)

[CVE-2021-4236](#) suppressed

Web Sockets do not execute any AuthenticateMethod methods which may be set, leading to a nil pointer dereference if the returned UserData pointer is assumed to be non-nil, or authentication bypass. This issue only affects WebSockets with an AuthenticateMethod hook. Request handlers that do not explicitly use WebSockets are not vulnerable.

#### CWE-476 NULL Pointer Dereference

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-2023-5072 - 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:

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

#### References:

- MISC - <https://github.com/ecnepsnai/web/commit/5a78f8d5c41ce60dcf9f61aaf47a7a8dc3e0002f>
- MISC - <https://pkg.go.dev/vuln/GO-2021-0107>

#### Vulnerable Software & Versions:

- [cpe:2.3:a:web\\_project:web:\\*:\\*:\\*:\\*:\\*go:\\* versions from \(including\) 1.4.0; versions up to \(excluding\) 1.5.2](#)

**taskplanner.zip: cron-utils.jar**

#### Description:

A Java library to parse, migrate and validate crons as well as describe them in human readable language

#### License:

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

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/taskplanner.zip/cron-utils.jar

**MD5:** 4c27537eecc6fa37ed5740b5383643c8

**SHA1:** 5d3738bc7a2eaa45a94a76c6e87af54a95414637

**SHA256:** 02af0e8b2fe93c9fa6eef97b53b39faae14c5b996356edb132e9fe620013744

#### Evidence



#### Suppressed Identifiers

- None

#### Suppressed Vulnerabilities



##### [CVE-2021-4277](#) suppressed

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

CWE-330 Use of Insufficiently Random Values

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 fredsmith, 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-2023-5072 - 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 (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:

- MISC - <https://github.com/fredsmith/utils/commit/dbab1b66955eeb3d76b34612b358307f5c4e3944>
- MISC - <https://vuldb.com/?id.216749>

Vulnerable Software & Versions:

- [cpe:2.3:a:utils\\_project:utils:\\*:\\*:\\*:\\*:\\* versions up to \(excluding\) 2021-05-14](#)

## theme.zip: bootstrap.jar: bootstrap.js

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/theme.zip/bootstrap.jar/META-INF/resources/webjars/bootstrap/3.4.1/js/bootstrap.js

**MD5:** 894d79839facf38d9fd672bdbe57443d

**SHA1:** 11277f4e04cf070a350e566b053ef2215993720c

**SHA256:** dbd2a35e72edc7d6bde483481a912f1c38aa57fab2747d9b071d317339ee03a2

### Evidence



### Related Dependencies



### Suppressed Identifiers

- None

### Suppressed Vulnerabilities



**Bootstrap before 4.0.0 is end-of-life and no longer maintained. (RETIREJS)** suppressed

Bootstrap before 4.0.0 is end-of-life and no longer maintained.

Notes: file name: remotegui.zip: bootstrap.jar

Unscored:

- Severity: low

References:

- info - <https://github.com/twbs/bootstrap/issues/20631>
- retid - 72

Vulnerable Software & Versions (RETIREJS):

## theme.zip: bootstrap.jar: bootstrap.min.js

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/theme.zip/bootstrap.jar/META-INF/resources/webjars/bootstrap/3.4.1/js/bootstrap.min.js

**MD5:** 2f34b630ffe30ba2ff2b91e3f3c322a1

**SHA1:** b16fd8226bd6bfb08e568f1b1d0a21d60247cefb

**SHA256:** 9ee2fcff6709e4d0d24b09ca0fc56aade12b4961ed9c43fd13b03248bfb57afe

### Evidence



### Related Dependencies





### Suppressed Identifiers

- None

### Suppressed Vulnerabilities



**Bootstrap before 4.0.0 is end-of-life and no longer maintained.** (RETIREJS) suppressed

Bootstrap before 4.0.0 is end-of-life and no longer maintained.

Notes: file name: remotegui.zip: bootstrap.jar

Unscored:

- Severity: low

References:

- info - <https://github.com/twbs/bootstrap/issues/20631>
- retid - 72

Vulnerable Software & Versions (RETIREJS):

## theme.zip: sass-compiler.jar

### Description:

A Sass compiler written completely in Java (pure Java).

### License:

The Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

**File Path:** /home/jenkins/workspace/helpdesk/Check-Product-Installer-for-Security-Problems/HelpDeskInstaller/server/build/tmp/dependencies/i-net HelpDesk/Server/plugins/theme.zip/sass-compiler.jar

**MD5:** ca4223e60127e6945b79f09280c9ce2b

**SHA1:** 1c3682c77fa0aa4bcc1b89fb18e3563987051f83

**SHA256:** 99dc28852324fd6f86441a92596f718a13be0e6b898b56b53f0d413768c5f415

### Evidence



### Suppressed Identifiers

- None

### Suppressed Vulnerabilities



[CVE-2019-10799](#) suppressed

compile-sass prior to 1.0.5 allows execution of arbitrary commands. The function "setupCleanupOnExit(cssPath)" within "dist/index.js" is executed as part of the "rm" command without any sanitization.

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

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 fredsmith, 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-2023-5072 - 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: HIGH (8.5)
- Vector: /AV:N/AC:L/Au:N/C:C/I:P/A:N

CVSSv3:

- HIGH (8.2)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

References:

- MISC - <https://github.com/eiskalteschatten/compile-sass/commit/d9ada7797ff93875b6466dea7a78768e90a0f8d2>
- MISC - <https://snyk.io/vuln/SNYK-JS-COMPILESASS-551804>

Vulnerable Software & Versions:

- [cpe:2.3:a:compile-sass\\_project:compile-sass:\\*:\\*:\\*:\\*:\\* versions up to \(excluding\) 1.0.5](#)

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](#).