



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: root project 'CoWorkInstaller'

cowork:CoWorkInstaller:25.4

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

- *dependency-check version:* 10.0.3
- *Report Generated On:* Thu, 3 Apr 2025 18:35:05 +0200
- *Dependencies Scanned:* 74 (73 unique)
- *Vulnerable Dependencies:* 0
- *Vulnerabilities Found:* 0
- *Vulnerabilities Suppressed:* 5 ([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



cowork.calls.zip: ice4j.jar

Description:

A Java implementation of the ICE protocol

License:

Apache-2.0: <https://github.com/jitsi/ice4j/blob/master/LICENSE>

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/ice4j.jar

MD5: 95ccd42c22c821a10722a74fb75d47f2

SHA1: 4fbe65fd307d75b45dd3e5710715124cb73e17bd

SHA256: 00b9cf7c274558de404c2d08f35de298541409eaf210994edb4c60b51a12757d

Referenced In Project/Scope: CoWorkInstaller

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-43550](#) suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), 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-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. 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 a CVE for a sample python project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. 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-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use.

CVSSv3:

- CRITICAL (9.8)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- support@hackerone.com - [PATCH](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:jitsi:jitsi:*:*:*:*:* versions up to \(excluding\) 2022-09-14](#)

cowork.calls.zip: jicoco-config.jar

Description:

Jitsi Common Components (Configuration Utilities)

License:

"Apache-2.0";link="https://github.com/jitsi/jicoco/blob/master/LICENSE"

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jicoco-config.jar
MD5: 2369693cf96dd817e1ddf46129143ad7
SHA1: d6602d58a4b13bbad51202338fa23ffc9595c707
SHA256: 9db4cc0c0d1985820c82895cffaf695a5d940db892c8e23d51cdce6d3c82a862
Referenced In Project/Scope: CoWorkInstaller

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-43550](#) suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), 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-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. 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 a CVE for a sample python project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. 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-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use.

CVSSv3:

- CRITICAL (9.8)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- support@hackerone.com - [PATCH](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:jitsi:jitsi:*.~*.~*.~*.~*.~*.~* versions up to \(excluding\) 2022-09-14](#)

cowork.calls.zip: jitsi-metaconfig.jar

Description:

jitsi-metaconfig helps solve the problems around the evolution of configuration properties

License:

Apache-2.0: <https://github.com/jitsi/jitsi-metaconfig/blob/master/LICENSE>

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jitsi-metaconfig.jar

MD5: 725b026d03d1dfcefb3ca4301f8d619a

SHA1: 20cf06693fec9f78466c21e15aa8b3f6b875f2f2

SHA256: 51802cbf89e0813cc3d59288eaf09d145101d874c8ca3433f968a4eb0c2c872a

Referenced In Project/Scope: CoWorkInstaller

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-43550](#) suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), 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-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. 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 a CVE for a sample python project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. 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-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use.

CVSSv3:

- CRITICAL (9.8)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- support@hackerone.com - [PATCH](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:jitsi:jitsi:*:*:*:*:* versions up to \(excluding\) 2022-09-14](#)

cowork.calls.zip: jitsi-utils.jar

Description:

A set of basic utilities used in Jitsi projects

License:

Apache-2.0: <https://github.com/jitsi/jitsi-utils/blob/master/LICENSE>

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jitsi-utils.jar

MD5: b2ca06a9a2e5e253298685fd3a38449c

SHA1: 20bb058007931515baf37d41e1cb252f88f56fa4

SHA256: 60503c6c694df00e5a878638198e8e54fdbcb0a6c7a28fd519940e2cbc593773c

Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- None

Suppressed Vulnerabilities

[CVE-2022-43550](#) suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), 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-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. 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 a CVE for a sample python project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. 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-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use.

CVSSv3:

- CRITICAL (9.8)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- support@hackerone.com - [PATCH](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:jitsi:jitsi:*:*:*:*:* versions up to \(excluding\) 2022-09-14](#)

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.zip/cowork-javadoc.jar/script-dir/jquery-ui.min.js

MD5: 32059df39c14a910ccc2325f6a3cd62f

SHA1: d3289f1b527a3f054d303ec769402e037fbfcf4b

SHA256: 672f278182cdf04f3c62a5b8d93f406791854a28791f27aecdb9981573c61424

Referenced In Project/Scope: CoWorkInstaller

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



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/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9>
- 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](#).