



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](#)

Project: project ':standalone'

pdfc:standalone:26.4

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

- *dependency-check version:* 12.2.1
- *Report Generated On:* Sat, 16 May 2026 17:50:38 +0200
- *Dependencies Scanned:* 130 (130 unique)
- *Vulnerable Dependencies:* 0
- *Vulnerabilities Found:* 0
- *Vulnerabilities Suppressed:* 6 ([show](#))
- ...

Analysis Exceptions

Failed to request component-reports. <https://ossindex.sonatype.org/api/v3/component-report> - Server status: 402 - Server reason: Payment Required



Failed to request component-reports. <https://ossindex.sonatype.org/api/v3/component-report> - Server status: 402 - Server reason: Payment Required



Failed to request component-reports. <https://ossindex.sonatype.org/api/v3/component-report> - Server status: 402 - Server reason: Payment Required



Failed to request component-reports. <https://ossindex.sonatype.org/api/v3/component-report> - Server status: 402 - Server reason: Payment Required



Failed to request component-reports. <https://ossindex.sonatype.org/api/v3/component-report> - Server status: 402 - Server reason: Payment Required



Failed to request component-reports. <https://ossindex.sonatype.org/api/v3/component-report> - Server status: 402 - Server reason: Payment Required



Failed to request component-reports. <https://ossindex.sonatype.org/api/v3/component-report> - Server status: 402 - Server reason: Payment Required





Summary

Summary of Vulnerable Dependencies [\(click to show all\)](#)

Dependency Vulnerability IDs Package Highest Severity CVE Count Confidence Evidence Count

Dependencies (vulnerable)

Suppressed Vulnerabilities



ocr.tesseract.zip: jbig2-imageio.jar

Description:

Java Image I/O plugin for reading JBIG2-compressed image data.
Formerly known as the levigo JBig2 ImageIO plugin (com.levigo.jbig2:levigo-jbig2-imageio).

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller
/standalone/build/tmp/dependencies/i-net PDFC/plugins/ocr.tesseract.zip/jbig2-imageio.jar

MD5: c51f45dc3d29bbf716774f9ff9e95ad6

SHA1: ad09a9bb94ea791ea81fb6c5bc2b13dd77872598

SHA256: 29cb2951622f10acf61fd0656c4e6fa5562194a9095f7a1d26aa426e2f6b17eb

Referenced In Project/Scope: standalone

Evidence



Suppressed Identifiers

- [cpe:2.3:a:apache:pdfbox:3.0.4:*.***.*.*](#) suppressed (Confidence: Highest)
 - Notes: Excluded due to not having a newer version available. This will be checked soon to mitigate. PDFBox is a tesseract dependency and not actively used in the product file name: ocr.tesseract.zip: jbig2-imageio.jar

Suppressed Vulnerabilities



[CVE-2026-23907](#) suppressed

This issue affects the
ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.35, from 3.0.0 through 3.0.6.

The ExtractEmbeddedFiles example contains a path traversal vulnerability (CWE-22) because the filename that is obtained from
PDComplexFileSpecification.getFilename() is appended to the extraction path.

Users who have copied this example into their production code should review it to ensure that the extraction path is acceptable. The example

has been changed accordingly, now the initial path and the extraction paths are converted into canonical paths and it is verified that extraction path contains the initial path. The documentation has also been adjusted.

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

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- security@apache.org - [MAILING_LIST,VENDOR_ADVISORY](#)
- security@apache.org - [NOT_APPLICABLE](#)

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

- [cpe:2.3:a:apache:pdfbox:*:*:*:*:* versions from \(including\) 3.0.0; versions up to \(including\) 3.0.7](#)
- ...

[CVE-2026-33929](#) suppressed

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache PDFBox Examples.

This issue affects the ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.36, from 3.0.0 through 3.0.7.

Users are recommended to update to version 2.0.37 or 3.0.8 once available. Until then, they should apply the fix provided in GitHub PR 427.

The ExtractEmbeddedFiles example contained a path traversal vulnerability (CWE-22) mentioned in CVE-2026-23907. However the change in the releases 2.0.36 and 3.0.7 is flawed because it doesn't consider the file path separator. Because of that, a user having writing rights on /home/ABC could be victim to a malicious PDF resulting in a write attempt to any path starting with /home/ABC, e.g. "/home/ABCDEF".

Users who have copied this example into their production code should apply the mentioned change. The example has been changed accordingly and is available in the project repository.

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

CVSSv3:

- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- security@apache.org - [MAILING_LIST](#)
- security@apache.org - [MAILING_LIST,VENDOR_ADVISORY](#)
- security@apache.org - [PATCH](#)

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

- [cpe:2.3:a:apache:pdfbox:*:*:*:*:* versions from \(including\) 3.0.0; versions up to \(excluding\) 3.0.8](#)
- ...

Description:

The Apache PDFBox library is an open source Java tool for working with PDF documents. This artefact contains the PDFDebugger.

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/standalone/build/tmp/dependencies/i-net PDFC/plugins/ocr.tesseract.zip/pdfbox-debugger.jar

MD5: 85573afca8351375b49718b379abc76c

SHA1: 2c48091b1dd9be69d09e1aea657fc1e4065b08e7

SHA256: 79320b36483f001661b01e9409d9b62066e07a3a4e2f9e6568d777b04896d130

Referenced In Project/Scope: standalone

Evidence

Suppressed Identifiers

- [cpe:2.3:a:apache:pdfbox:3.0.7:*:*:*:*:*](#) suppressed (*Confidence:*Highest)
 - Notes: Excluded due to not having a newer version available. This will be checked soon to mitigate. PDFBox is a tesseract dependency and not actively used in the product file name: ocr.tesseract.zip: pdfbox-debugger.jar

Suppressed Vulnerabilities

[CVE-2026-23907](#) suppressed

This issue affects the ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.35, from 3.0.0 through 3.0.6.

The ExtractEmbeddedFiles example contains a path traversal vulnerability (CWE-22) because the filename that is obtained from `PDComplexFileSpecification.getFilename()` is appended to the extraction path.

Users who have copied this example into their production code should review it to ensure that the extraction path is acceptable. The example has been changed accordingly, now the initial path and the extraction paths are converted into canonical paths and it is verified that extraction path contains the initial path. The documentation has also been adjusted.

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

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- security@apache.org - [MAILING_LIST,VENDOR_ADVISORY](#)
- security@apache.org - [NOT_APPLICABLE](#)

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

- [cpe:2.3:a:apache:pdfbox:*:*:*:*:* versions from \(including\) 3.0.0; versions up to \(including\) 3.0.7](#)
- ...

[CVE-2026-33929](#) suppressed

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache PDFBox Examples.

This issue affects the ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.36, from 3.0.0 through 3.0.7.

Users are recommended to update to version 2.0.37 or 3.0.8 once available. Until then, they should apply the fix provided in GitHub PR 427.

The ExtractEmbeddedFiles example contained a path traversal vulnerability (CWE-22) mentioned in CVE-2026-23907. However the change in the releases 2.0.36 and 3.0.7 is flawed because it doesn't consider the file path separator. Because of that, a user having writing rights on /home/ABC could be victim to a malicious PDF resulting in a write attempt to any path starting with /home/ABC, e.g. "/home/ABCDEF".

Users who have copied this example into their production code should apply the mentioned change. The example has been changed accordingly and is available in the project repository.

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

CVSSv3:

- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- security@apache.org - [MAILING_LIST](#)
- security@apache.org - [MAILING_LIST,VENDOR_ADVISORY](#)
- security@apache.org - [PATCH](#)

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

- [cpe:2.3:a:apache:pdfbox:*:*:*:*:* versions from \(including\) 3.0.0; versions up to \(excluding\) 3.0.8](#)
- ...

ocr.tesseract.zip: pdfbox.jar

Description:

The Apache PDFBox library is an open source Java tool for working with PDF documents.

License:

<https://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/standalone/build/tmp/dependencies/i-net PDFC/plugins/ocr.tesseract.zip/pdfbox.jar

MD5: adeb0637e9451d49e610ee3bc16781cd

SHA1: ecfc1bbfa656d3e330b8cc9e6996a18cde1c9bd0

SHA256: 7cefa717622330951b4343abf1e5d36bccb11f4ba245d78aaa73251d08fec623

Referenced In Project/Scope: standalone

Evidence

Suppressed Identifiers

- [cpe:2.3:a:apache:pdfbox:3.0.7:*:*:*:*:*](#) suppressed (*Confidence:*Highest)
 - Notes: Excluded due to not having a newer version available. This will be checked soon to mitigate. PDFBox is a tesseract dependency and not actively used in the product file name: ocr.tesseract.zip: pdfbox.jar

Suppressed Vulnerabilities

[CVE-2026-23907](#) suppressed

This issue affects the ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.35, from 3.0.0 through 3.0.6.

The ExtractEmbeddedFiles example contains a path traversal vulnerability (CWE-22) because the filename that is obtained from `PDComplexFileSpecification.getFilename()` is appended to the extraction path.

Users who have copied this example into their production code should review it to ensure that the extraction path is acceptable. The example has been changed accordingly, now the initial path and the extraction paths are converted into canonical paths and it is verified that extraction path contains the initial path. The documentation has also been adjusted.

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

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- security@apache.org - [MAILING_LIST,VENDOR_ADVISORY](#)
- security@apache.org - [NOT_APPLICABLE](#)

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

- [cpe:2.3:a:apache:pdfbox:*:*:*:*:*](#) versions from (including) 3.0.0; versions up to (including) 3.0.7
- ...

[CVE-2026-33929](#) suppressed

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache PDFBox Examples.

This issue affects the ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.36, from 3.0.0 through 3.0.7.

Users are recommended to update to version 2.0.37 or 3.0.8 once available. Until then, they should apply the fix provided in GitHub PR 427.

The ExtractEmbeddedFiles example contained a path traversal vulnerability (CWE-22) mentioned in CVE-2026-23907. However the change in the releases 2.0.36 and 3.0.7 is flawed because it doesn't consider the file path separator. Because of that, a user having writing rights on /home/ABC could be victim to a malicious PDF resulting in a write attempt to any path starting with /home/ABC, e.g. "/home/ABCDEF".

Users who have copied this example into their production code should apply the mentioned change. The example has been changed accordingly and is available in the project repository.

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

CVSSv3:

- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

- security@apache.org - [MAILING_LIST](#)
- security@apache.org - [MAILING_LIST,VENDOR_ADVISORY](#)
- security@apache.org - [PATCH](#)

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

- [cpe:2.3:a:apache:pdfbox:*:*:*:*:* versions from \(including\) 3.0.0; versions up to \(excluding\) 3.0.8](#)
- ...

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](#).