



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*: Fri, 7 Aug 2026 20:09:56 +0200
- *Dependencies Scanned*: 1471 (1395 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 146 ([show](#))
- ...

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/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/>
- 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/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/>
- 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; versions of the package angularjs 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 - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616>
- 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-2026-11998](#) (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- info - <https://access.redhat.com/security/cve/CVE-2026-11998>
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - <https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8>
- info - <https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs>

Vulnerable Software & Versions (RETIREJS):

[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-2gqx-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-animate.jar: angular-animate.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-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/angular-animate.min.js

MD5: 5d2d0f42bb7e1b5503e914674f59dad0

SHA1: 4c15a58541e53c451c6f946d2048104f88b833c7

SHA256: 8e6202b1330a469a61ccdeebbd1cb3a20d0ecdffc8d106f68da5b85e9b67a1cd5

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; versions of the package angularjs 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 - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616>
- 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-2026-11998 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- info - <https://access.redhat.com/security/cve/CVE-2026-11998>
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - <https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8>
- info - <https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs>

Vulnerable Software & Versions (RETIREJS):

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](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-mqmq9-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/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/>
- 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/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/>
- 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; versions of the package angularjs 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 - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616>
- 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-2026-11998 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- info - <https://access.redhat.com/security/cve/CVE-2026-11998>
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - <https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8>
- info - <https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs>

Vulnerable Software & Versions (RETIREJS):

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-2gqx-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](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.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/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/>
- 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/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/>
- 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; versions of the package angularjs 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 - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616>
- 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-2026-11998 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- info - <https://access.redhat.com/security/cve/CVE-2026-11998>
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - <https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8>
- info - <https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs>

Vulnerable Software & Versions (RETIREJS):

[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](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-mqgm9-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-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; versions of the package angularjs 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 - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616>
- 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-2026-11998 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- info - <https://access.redhat.com/security/cve/CVE-2026-11998>
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - <https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8>
- info - <https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs>

Vulnerable Software & Versions (RETIREJS):

[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](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.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

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:

- [illegible]

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; versions of the package angularjs 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 - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616>
- 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-2026-11998](#) (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- info - <https://access.redhat.com/security/cve/CVE-2026-11998>
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - <https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8>
- info - <https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs>

Vulnerable Software & Versions (RETIREJS):

[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](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.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

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/2WUSPYOTOMAZPDEFPPWSPSCSPMNODRDKK3/>
- 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/2WUSPYOTOMAZPDEFPPWSPSCSPMNODRDKK3/>
- 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; versions of the package angularjs 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 - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616>
- 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](#)
- report@snyk.io - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- info - <https://access.redhat.com/security/cve/CVE-2026-11998>
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - <https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8>
- info - <https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs>

Vulnerable Software & Versions (RETIREJS):

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-gwqh-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](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.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/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/>
- 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/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/>
- 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; versions of the package angularjs 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 - <https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616>
- 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-2026-11998 (RETIREJS) suppressed

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- info - <https://access.redhat.com/security/cve/CVE-2026-11998>
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - <https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8>
- info - <https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998>
- info - <https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs>

Vulnerable Software & Versions (RETIREJS):

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-2gqx-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](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: 54aae4c54cceb8eea1b3b9f74d958d813a113a3

SHA256: b366d47bca68c558550a58193bd4a1e05a1f5ef98cbaab316e392937da38f3eb

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2026-49978](#) suppressed

DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Prior to 3.4.7, DOMPurify IN_PLACE sanitization could skip shadow contents attached to an element inside <template>.content, allowing attacker-controlled markup such as event handlers, JavaScript URLs, or scripts to survive and execute when an application cloned and inserted the sanitized template. This issue is fixed in version 3.4.7.

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/206>

CVSSv4:

- MEDIUM (6.3)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:H/SI:H/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,VENDOR_ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-rp9w-3fw7-7cwq>
- security-advisories@github.com - [EXPLOIT,VENDOR_ADVISORY](#)
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [RELEASE_NOTES](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.7

[CVE-2026-49458](#) suppressed

DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Prior to 3.4.6, DOMPurify.sanitize(node, { IN_PLACE: true }) accepted same-origin foreign-realm DOM nodes while follow-on checks used parent-realm constructors, causing instanceof checks for forms, named node maps, document fragments, and elements to fail and skip clobber, template-content, and shadow-DOM sanitization branches so executable markup could survive. This issue is fixed in version 3.4.6.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), CWE-501 Trust Boundary Violation, CWE-693 Protection Mechanism Failure

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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,VENDOR_ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-hpcv-96wg-7vj8>
- security-advisories@github.com - [EXPLOIT,MITIGATION,VENDOR_ADVISORY](#)
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [RELEASE_NOTES](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.6

[CVE-2026-49459](#) suppressed

DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Prior to 3.4.6, DOMPurify.sanitize(root, { IN_PLACE: true }) could preserve event-handler attributes on an attacker-controlled <form> root when a descendant name clobbered properties checked by _isClobbered, because _forceRemove no-opped on the parent-less root and _sanitizeAttributes returned early. This issue is fixed in version 3.4.6.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), CWE-1321 Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution'), CWE-693 Protection Mechanism Failure

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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,VENDOR_ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-r47g-fvhr-h676>
- security-advisories@github.com - [EXPLOIT,MITIGATION,VENDOR_ADVISORY](#)
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [RELEASE_NOTES](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.6

[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/206>

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/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:

- 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/206>

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-2026-65902](#) suppressed

DOMPurify before 3.4.7 (affected versions <= 3.4.5) passes direct references to the module-level DEFAULT_ALLOWED_TAGS and DEFAULT_ALLOWED_ATTR sets to the uponSanitizeElement and uponSanitizeAttribute hooks via data.allowedTags / data.allowedAttributes when sanitize is called without an explicit cfg.ALLOWED_TAGS / cfg.ALLOWED_ATTR array. A hook that mutates these fields permanently widens the default allow-lists for the lifetime of the DOMPurify instance, so all subsequent default-config sanitize calls inherit the widened defaults and attacker payloads using the poisoned tag/attribute name survive sanitization. removeAllHooks(), clearConfig(), and passing a fresh cfg do not recover the state; only constructing a new DOMPurify instance does.

CWE-501 Trust Boundary Violation

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

CVSSv4:

- MEDIUM (5.3)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/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:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [PATCH](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-76mc-f452-cxcm>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.7

[CVE-2026-65914](#) suppressed

DOMPurify before 3.3.2 contains a mutation-XSS vulnerability when sanitized HTML is reinserted into special parsing contexts using innerHTML with wrappers like script, xmp, iframe, noembed, noframes, or noscript. Attackers can craft payloads with closing sequences that break out of the wrapper context during reparsing, reactivating dangerous markup with event handlers to execute JavaScript.

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/206>

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/RS: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,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- 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 (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.3.2

[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/206>

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/RS: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

[CVE-2026-65898](#) suppressed

DOMPurify before 3.4.11 fails to clone the ALLOWED_ATTR allowlist when setConfig() is used with an uponSanitizeAttribute hook, allowing the hook to permanently mutate the shared allowlist. Attackers can register a hook that conditionally allows dangerous attributes like onerror for trusted elements, then submit untrusted content that inherits the polluted allowlist and executes event handlers as stored XSS.

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/206>

CVSSv4:

- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:L/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:

- HIGH (7.2)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-cmwh-pvxp-8882>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.11

[CVE-2026-65899](#) suppressed

DOMPurify 3.0.0 before 3.4.9 does not reset the retained Trusted Types policy when clearConfig() is called, so a DOMPurify instance reused across trust boundaries stays bound to a previously supplied TRUSTED_TYPES_POLICY. A later caller that requests RETURN_TRUSTED_TYPE output receives a TrustedHTML object created by the old (potentially unsafe) policy rather than a clean default, which can lead to script execution at a Trusted Types sink. Passing TRUSTED_TYPES_POLICY: null on the later call also does not clear the retained policy.

CWE-693 Protection Mechanism Failure

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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 - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [PATCH](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-vxr8-fq34-vvx9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 3.0.0; versions up to (excluding) 3.4.9

[CVE-2026-65900](#) suppressed

DOMPurify versions >=3.0.0 and before 3.4.8, when configured with SAFE_FOR_TEMPLATES together with a DOM output mode (RETURN_DOM, RETURN_DOM_FRAGMENT, or IN_PLACE), fail to strip template expressions (e.g. \${evil}, {{evil}}, <%evil%>) inside <template> element content. The final normalization/scrub pass (_scrubTemplateExpressions) uses a NodeIterator and node.normalize() that do not descend into template.content, so expressions

that only form after adjacent text nodes merge survive sanitization. This bypasses SAFE_FOR_TEMPLATES and can allow a downstream template engine to evaluate attacker-supplied expressions. The string output path is not affected.

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/206>

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/IS: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,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-gvmj-g25r-r7wr>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 3.0.0; versions up to (excluding) 3.4.8

[CVE-2026-65901](#) suppressed

DOMPurify through 3.4.6 contains a cross-site scripting vulnerability in IN_PLACE mode that trusts attacker-controlled nodeName on live non-form nodes. Attackers can supply hostile live DOM objects with real script children whose observable nodeName is clobbered to appear as allowed elements, causing scripts to execute when the sanitized tree is inserted into a live document.

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/206>

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/IS: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,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-x4vx-rjvf-j5p4>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.7

[CVE-2026-65903](#) suppressed

DOMPurify before 3.4.0 contains a logic error in the ADD_TAGS function where short-circuit evaluation allows forbidden tags to bypass FORBID_TAGS restrictions. Attackers can craft input containing tags listed in FORBID_TAGS that are also added via ADD_TAGS function, causing them to be retained in sanitized output.

CWE-697 Incorrect Comparison

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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 - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-39q2-94rc-95cp>

Vulnerable Software & Versions (NVD):

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

[CVE-2026-65912](#) suppressed

DOMPurify before 3.3.2 contains a URI validation bypass vulnerability when ADD_ATTR is provided as a predicate function via EXTRA_ELEMENT_HANDLING.attributeCheck. Attackers can supply a predicate that accepts specific attribute and tag combinations to bypass URI-safe validation, allowing unsafe protocols like javascript: to survive sanitization and execute as DOM-based XSS when the link is activated.

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/206>

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 - [THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- 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 (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.3.2

[CVE-2026-65913](#) suppressed

DOMPurify before 3.3.2 contains a prototype pollution vulnerability in USE_PROFILES mode that allows attackers to bypass attribute filtering by polluting Array.prototype properties. Attackers can set Array.prototype properties like onclick to true, causing DOMPurify to accept event handlers as allowlisted attributes and resulting in DOM-based XSS when sanitized markup is rendered.

CWE-1321 Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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/RS: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 - [THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- 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 (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.3.2

[CVE-2026-66010](#) suppressed

DOMPurify before 3.4.12 fails to execute afterSanitizeElements hook for custom elements allowed via CUSTOM_ELEMENT_HANDLING.tagNameCheck, allowing attributes to bypass application security policies. Attackers can preserve sensitive attributes on custom elements that later re-inject them into innerHTML sinks, creating second-order XSS gadgets.

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/206>

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/RS: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,VENDOR ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,VENDOR ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197>
- info - <https://github.com/cure53/DOMPurify/pull/1537>
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.4.12>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.12

[CVE-2026-41238](#) (RETIREJS) suppressed

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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/206>

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-2026-49978](#) suppressed

DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Prior to 3.4.7, DOMPurify IN_PLACE sanitization could skip shadow contents attached to an element inside <template>.content, allowing attacker-controlled markup such as event handlers, JavaScript URLs, or scripts to survive and execute when an application cloned and inserted the sanitized template. This issue is fixed in version 3.4.7.

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/206>

CVSSv4:

- MEDIUM (6.3)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:H/SI:H/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,VENDOR ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-rp9w-3fw7-7cwq>
- security-advisories@github.com - [EXPLOIT,VENDOR ADVISORY](#)
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [RELEASE NOTES](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.7

[CVE-2026-49458](#) suppressed

DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Prior to 3.4.6, DOMPurify.sanitize(node, { IN_PLACE: true }) accepted same-origin foreign-realm DOM nodes while follow-on checks used parent-realm constructors, causing instanceof checks for forms, named node maps, document fragments, and elements to fail and skip clobber, template-content, and shadow-DOM sanitization branches so executable markup could survive. This issue is fixed in version 3.4.6.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), CWE-501 Trust Boundary Violation, CWE-693 Protection Mechanism Failure

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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,VENDOR ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-hpcv-96wg-7vj8>
- security-advisories@github.com - [EXPLOIT,MITIGATION,VENDOR ADVISORY](#)
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [RELEASE NOTES](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.6

[CVE-2026-49459](#) suppressed

DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Prior to 3.4.6, DOMPurify.sanitize(root, { IN_PLACE: true }) could preserve event-handler attributes on an attacker-controlled <form> root when a descendant name clobbered properties checked by _isClobbered, because _forceRemove no-opped on the parent-less root and _sanitizeAttributes returned early. This issue is fixed in version 3.4.6.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), CWE-1321 Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution'), CWE-693 Protection Mechanism Failure

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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,VENDOR ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-r47g-fvhr-h676>
- security-advisories@github.com - [EXPLOIT,MITIGATION,VENDOR ADVISORY](#)
- security-advisories@github.com - [PATCH](#)

- security-advisories@github.com - [RELEASE NOTES](#)

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.6

[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/206>

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/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:

- 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/206>

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-2026-65902](#) suppressed

DOMPurify before 3.4.7 (affected versions <= 3.4.5) passes direct references to the module-level DEFAULT_ALLOWED_TAGS and DEFAULT_ALLOWED_ATTR sets to the uponSanitizeElement and uponSanitizeAttribute hooks via data.allowedTags / data.allowedAttributes when sanitize is called without an explicit cfg.ALLOWED_TAGS / cfg.ALLOWED_ATTR array. A hook that mutates these fields permanently widens the default allow-lists for the lifetime of the DOMPurify instance, so all subsequent default-config sanitize calls inherit the widened defaults and attacker payloads using the poisoned tag/attribute name survive sanitization. removeAllHooks(), clearConfig(), and passing a fresh cfg do not recover the state; only constructing a new DOMPurify instance does.

CWE-501 Trust Boundary Violation

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

CVSSv4:

- MEDIUM (5.3)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/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:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [PATCH](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-76mc-f452-cxcm>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.7

[CVE-2026-65914](#) suppressed

DOMPurify before 3.3.2 contains a mutation-XSS vulnerability when sanitized HTML is reinserted into special parsing contexts using innerHTML with wrappers like script, xmp, iframe, noembed, noframes, or noscript. Attackers can craft payloads with closing sequences that break out of the wrapper context during reparsing, reactivating dangerous markup with event handlers to execute JavaScript.

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/206>

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:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- disclosure@vulncheck.com - [THIRD_PARTY_ADVISORY](#)
- 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 (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.3.2

[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/206>

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/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

[CVE-2026-65898](#) suppressed

DOMPurify before 3.4.11 fails to clone the ALLOWED_ATTR allowlist when setConfig() is used with an uponSanitizeAttribute hook, allowing the hook to permanently mutate the shared allowlist. Attackers can register a hook that conditionally allows dangerous attributes like onerror

for trusted elements, then submit untrusted content that inherits the polluted allowlist and executes event handlers as stored XSS.

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/206>

CVSSv4:

- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:L/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:

- HIGH (7.2)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-cmwh-pvxp-8882>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.11

[CVE-2026-65899](#) suppressed

DOMPurify 3.0.0 before 3.4.9 does not reset the retained Trusted Types policy when `clearConfig()` is called, so a DOMPurify instance reused across trust boundaries stays bound to a previously supplied `TRUSTED_TYPES_POLICY`. A later caller that requests `RETURN_TRUSTED_TYPE` output receives a `TrustedHTML` object created by the old (potentially unsafe) policy rather than a clean default, which can lead to script execution at a Trusted Types sink. Passing `TRUSTED_TYPES_POLICY: null` on the later call also does not clear the retained policy.

CWE-693 Protection Mechanism Failure

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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 - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [PATCH](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-vxr8-fq34-vvx9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 3.0.0; versions up to (excluding) 3.4.9

[CVE-2026-65900](#) suppressed

DOMPurify versions $\geq 3.0.0$ and before 3.4.8, when configured with `SAFE_FOR_TEMPLATES` together with a DOM output mode (`RETURN_DOM`, `RETURN_DOM_FRAGMENT`, or `IN_PLACE`), fail to strip template expressions (e.g. `${evil}`, `{{evil}}`, `<%evil%>`) inside `<template>` element content. The final normalization/scrub pass (`_scrubTemplateExpressions`) uses a

NodeIterator and node.normalize() that do not descend into template.content, so expressions that only form after adjacent text nodes merge survive sanitization. This bypasses SAFE_FOR_TEMPLATES and can allow a downstream template engine to evaluate attacker-supplied expressions. The string output path is not affected.

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/206>

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/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,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-gvmj-g25r-r7wr>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions from (including) 3.0.0; versions up to (excluding) 3.4.8

[CVE-2026-65901](#) suppressed

DOMPurify through 3.4.6 contains a cross-site scripting vulnerability in IN_PLACE mode that trusts attacker-controlled nodeName on live non-form nodes. Attackers can supply hostile live DOM objects with real script children whose observable nodeName is clobbered to appear as allowed elements, causing scripts to execute when the sanitized tree is inserted into a live document.

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/206>

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/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,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-x4vx-rjvf-j5p4>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.7

[CVE-2026-65903](#) suppressed

DOMPurify before 3.4.0 contains a logic error in the ADD_TAGS function where short-circuit evaluation allows forbidden tags to bypass FORBID_TAGS restrictions. Attackers can craft input containing tags listed in FORBID_TAGS that are also added via ADD_TAGS function, causing them to be retained in sanitized output.

CWE-697 Incorrect Comparison

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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 - [EXPLOIT,THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-39q2-94rc-95cp>

Vulnerable Software & Versions (NVD):

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

[CVE-2026-65912](#) suppressed

DOMPurify before 3.3.2 contains a URI validation bypass vulnerability when ADD_ATTR is provided as a predicate function via EXTRA_ELEMENT_HANDLING.attributeCheck. Attackers can supply a predicate that accepts specific attribute and tag combinations to bypass URI-safe validation, allowing unsafe protocols like javascript: to survive sanitization and execute as DOM-based XSS when the link is activated.

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/206>

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 - [THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- 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 (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.3.2

[CVE-2026-65913](#) suppressed

DOMPurify before 3.3.2 contains a prototype pollution vulnerability in USE_PROFILES mode that allows attackers to bypass attribute filtering by polluting Array.prototype properties. Attackers can set Array.prototype properties like onclick to true, causing DOMPurify to accept event handlers as allowlisted attributes and resulting in DOM-based XSS when sanitized markup is rendered.

CWE-1321 Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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 - [THIRD PARTY ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- 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 (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.3.2

[CVE-2026-66010](#) suppressed

DOMPurify before 3.4.12 fails to execute afterSanitizeElements hook for custom elements allowed via CUSTOM_ELEMENT_HANDLING.tagNameCheck, allowing attributes to bypass application security policies. Attackers can preserve sensitive attributes on custom elements that later re-inject them into innerHTML sinks, creating second-order XSS gadgets.

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/206>

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:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT,VENDOR ADVISORY](#)
- disclosure@vulncheck.com - [EXPLOIT,VENDOR ADVISORY](#)
- disclosure@vulncheck.com - [THIRD PARTY ADVISORY](#)
- info - <https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197>
- info - <https://github.com/cure53/DOMPurify/pull/1537>
- info - <https://github.com/cure53/DOMPurify/releases/tag/3.4.12>
- info - <https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:cure53:dompurify:*:*:*:*:* versions up to (excluding) 3.4.12

[CVE-2026-41238](#) (RETIREJS) suppressed

Notes: HugeRTE: There is currently no fixed date. <https://github.com/hugerte/hugerte/issues/206>

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/206>

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](#).