



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

 [Sponsor](#)

Project: project ':server'

clear-reports:server:24.4

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

- *dependency-check version:* 8.4.0
- *Report Generated On:* Tue, 21 May 2024 18:56:57 +0200
- *Dependencies Scanned:* 1513 (1364 unique)
- *Vulnerable Dependencies:* 1
- *Vulnerabilities Found:* 1
- *Vulnerabilities Suppressed:* 70 ([show](#))
- ...

Summary

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

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
remotegui.zip: jquery.jar		pkg: javascript/jquery@2.2.4 pkg: maven/org.webjars/jquery@2.2.4	HIGH	1		17

Dependencies (vulnerable)

remotegui.zip: jquery.jar

Description:

WebJar for jQuery

License:

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/remotegui.zip/jquery.jar
MD5: 4af65e569248d8a2411f66498d720280
SHA1: c3dc40b1b5f24c56afa36fd9a463bb9f378ac4ab
SHA256: de28c4da0ea9f16101352dd3582ec8021ee5e2de5f45104ca171876003d54db6
Referenced In Project/Scope: server

Evidence

Identifiers

- [pkg:javascript/jquery@2.2.4](#) (Confidence: Highest)
- [pkg:maven/org.webjars/jquery@2.2.4](#) (Confidence: High)

Published Vulnerabilities

CVE-2016-10707 (OSSINDEX) suppress

jquery - Uncontrolled Resource Consumption

The software does not properly restrict the size or amount of resources that are requested or influenced by an actor, which can be used to consume more resources than intended.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2016-10707> for details

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:

- OSSINDEX - [\[CVE-2016-10707\] CWE-400: Uncontrolled Resource Consumption \('Resource Exhaustion'\)](#)
- OSSIndex - <https://github.com/advisories/GHSA-mhpp-875w-9cpv>
- OSSIndex - <https://github.com/jquery/jquery/issues/3133>
- OSSIndex - <https://github.com/jquery/jquery/issues/3371>
- OSSIndex - <https://github.com/jquery/jquery/pull/2916>
- OSSIndex - <https://github.com/jquery/jquery/pull/3134>

Vulnerable Software & Versions (OSSINDEX):

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

Suppressed Vulnerabilities

authentication.oauth.zip: authentication.oauth-javadoc.jar: jquery-ui.min.js

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/authentication.oauth.zip/authentication.oauth-javadoc.jar/script-dir/jquery-ui.min.js

MD5: 32059df39c14a910ccc2325f6a3cd62f

SHA1: d3289f1b527a3f054d303ec769402e037fbcf4b

SHA256: 672f278182cdf04f3c62a5b8d93f406791854a28791f27aecdb9981573c61424

Referenced In Project/Scope: server

Evidence



Related Dependencies



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-31160](#) suppressed

jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-site scripting. Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. Calling `.checkboxradio("refresh")` on such a widget and the initial HTML contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery UI 1.13.2. To remediate the issue, someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.

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

Notes: JavaDoc embedded JQuery UI - requires updated Java Version with newer javadoc

CVSSv3:

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

References:

- - [FEDORA-2022-1a01ed37e2](#)
- - [FEDORA-2022-22d8ba36d0](#)
- - [FEDORA-2022-7291b78111](#)
- CONFIRM - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-h6gj-6jjq-h8g9>
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220909-0007/>
- MISC - <https://blog.jqueryui.com/2022/07/jquery-ui-1-13-2-released/>
- MISC - <https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9>
- MISC - <https://www.drupal.org/sa-contrib-2022-052>
- MLIST - [\[debian-lts-announce\] 20221207 \[SECURITY\] \[DLA 3230-1\] jqueryui security update](#)
- info - <https://github.com/advisories/GHSA-h6gj-6jjq-h8g9>
- info - <https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9>
- info - <https://github.com/jquery/jquery-ui/issues/2101>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2022-31160>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:drupal:jquery_ui_checkboxradio:8.x-1.0:*:*:*:*:drupal:*.*
- cpe:2.3:a:drupal:jquery_ui_checkboxradio:8.x-1.1:*:*:*:*:drupal:*.*
- cpe:2.3:a:drupal:jquery_ui_checkboxradio:8.x-1.2:*:*:*:*:drupal:*.*
- cpe:2.3:a:drupal:jquery_ui_checkboxradio:8.x-1.3:*:*:*:*:drupal:*.*

- cpe:2.3:a:jqueryui:jquery_ui:*:*:*:*:*:jquery:*:* versions up to (excluding) 1.13.2
- cpe:2.3:a:netapp:oncommand_insight:*:*:*:*:*:

docfx.vendor.js

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/Documentation and Samples/dotnet - ProcessBridge API Doc/styles/docfx.vendor.js

MD5: e546d4a3ac43d85422e9c43bf9488c88

SHA1: 7387f5bf1a3382308d646560039243629968f137

SHA256: 4dfa2ef41a41c02b0cd0cb18b5c3ee71dd40cdc060271f0d832235e7a1c72c34

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



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

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

Notes: file name: remotegui.zip: bootstrap.jar We are in the process of migrating required functions into a custom framework.

Unscored:

- Severity: low

References:

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

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/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

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

CVSSv2:

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

CVSSv3:

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

References:

- - [FEDORA-2022-e016e6f445](#)
- - [FEDORA-2022-edf635cf39](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220629-0009/>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2772736>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2772738>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2772737>
- MISC - <https://snyk.io/vuln/SNYK-JS-ANGULAR-2772735>
- MISC - <https://stackblitz.com/edit/angularjs-material-blank-zvtdvb>
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

[CVE-2024-21490](#) suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- - <https://support.heroku.com/hc/en-us/articles/25715686953485-CVE-2024-21490-AngularJS-Regular-Expression-Denial-of-Service-ReDoS>
- 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>

Vulnerable Software & Versions (NVD):

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

[CVE-2022-25869](#) suppressed

All versions of package angular 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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*

[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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406320>

- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406322>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406321>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos>
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406323>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406325>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406324>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373045>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-resource-trailing-slashes-redos>
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406326>

- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406328>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406327>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373046>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos>
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>

Vulnerable Software & Versions (NVD):

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

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://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/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

CVSSv2:

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

CVSSv3:

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

References:

- - [FEDORA-2022-e016e6f445](#)
- - [FEDORA-2022-edf635cf39](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220629-0009/>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2772736>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2772738>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2772737>
- MISC - <https://snyk.io/vuln/SNYK-JS-ANGULAR-2772735>
- MISC - <https://stackblitz.com/edit/angularjs-material-blank-zvtdvb>
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*:

[CVE-2024-21490](#) suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- - <https://support.heroku.com/hc/en-us/articles/25715686953485-CVE-2024-21490-AngularJS-Regular-Expression-Denial-of-Service-ReDoS>
- 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>

Vulnerable Software & Versions (NVD):

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

[CVE-2022-25869](#) suppressed

All versions of package angular 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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:*

[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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406320>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406322>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406321>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos>
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406323>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406325>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406324>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373045>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-resource-trailing-slashes-redos>
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406326>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406328>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406327>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373046>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos>
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>

Vulnerable Software & Versions (NVD):

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

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://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/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

CVSSv2:

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

CVSSv3:

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

References:

- - [FEDORA-2022-e016e6f445](#)
- - [FEDORA-2022-edf635cf39](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220629-0009/>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2772736>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2772738>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2772737>
- MISC - <https://snyk.io/vuln/SNYK-JS-ANGULAR-2772735>
- MISC - <https://stackblitz.com/edit/angularjs-material-blank-zvtdvb>

- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*

[CVE-2024-21490](#) suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- - <https://support.heroku.com/hc/en-us/articles/25715686953485-CVE-2024-21490-AngularJS-Regular-Expression-Denial-of-Service-ReDoS>
- 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>

Vulnerable Software & Versions (NVD):

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

[CVE-2022-25869](#) suppressed

All versions of package angular 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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:*

[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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406320>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406322>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406321>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos>
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406323>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406325>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406324>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373045>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-resource-trailing-slashes-redos>
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406326>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406328>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406327>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373046>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos>
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>

Vulnerable Software & Versions (NVD):

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

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://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/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

CVSSv2:

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

CVSSv3:

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

References:

- - [FEDORA-2022-e016e6f445](#)
- - [FEDORA-2022-edf635cf39](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220629-0009/>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2772736>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2772738>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2772737>
- MISC - <https://snyk.io/vuln/SNYK-JS-ANGULAR-2772735>
- MISC - <https://stackblitz.com/edit/angularjs-material-blank-zvtdvb>
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

[CVE-2024-21490](#) suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- - <https://support.heroku.com/hc/en-us/articles/25715686953485-CVE-2024-21490-AngularJS-Regular-Expression-Denial-of-Service-ReDoS>
- 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>

Vulnerable Software & Versions (NVD):

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

[CVE-2022-25869](#) suppressed

All versions of package angular 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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*

[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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406320>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406322>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406321>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>

- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos>
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406323>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406325>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406324>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373045>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-resource-trailing-slashes-redos>
- info - <https://github.com/advisories/GHSA-2qqx-w9hr-q5gx>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406326>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406328>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406327>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373046>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos>

- info - <https://github.com/advisories/GHSA-gwqh-hm9m-p5hr>

Vulnerable Software & Versions (NVD):

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

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://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/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

CVSSv2:

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

CVSSv3:

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

References:

- - [FEDORA-2022-e016e6f445](#)
- - [FEDORA-2022-edf635cf39](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220629-0009/>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2772736>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2772738>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2772737>
- MISC - <https://snyk.io/vuln/SNYK-JS-ANGULAR-2772735>
- MISC - <https://stackblitz.com/edit/angularjs-material-blank-zvtdvb>
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

[CVE-2024-21490](#) suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- - <https://support.herodevs.com/hc/en-us/articles/25715686953485-CVE-2024-21490-AngularJS-Regular-Expression-Denial-of-Service-ReDoS>
- 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>

Vulnerable Software & Versions (NVD):

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

[CVE-2022-25869](#) suppressed

All versions of package angular 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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:*

[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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406320>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406322>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406321>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos>
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406323>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406325>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406324>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373045>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-resource-trailing-slashes-redos>
- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406326>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406328>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406327>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373046>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos>
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>

Vulnerable Software & Versions (NVD):

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

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://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>
- retid - 54

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

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

MD5: f3c62abeec216e9431e7d5b22d8e813b

SHA1: 21355ef18c5e1ce2b2c711b9dba21cbea0655646

SHA256: cc80a30ad0439c2e9c209b3d7fcffb1d10e6007fd1d00c9cc144f393664a7045

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2022-25844](#) suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv2:

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

CVSSv3:

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

References:

- - [FEDORA-2022-e016e6f445](#)
- - [FEDORA-2022-edf635cf39](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220629-0009/>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2772736>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2772738>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2772737>
- MISC - <https://snyk.io/vuln/SNYK-JS-ANGULAR-2772735>
- MISC - <https://stackblitz.com/edit/angularjs-material-blank-zvtdvb>
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*:

[CVE-2024-21490](#) suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- - <https://support.heroku.com/hc/en-us/articles/25715686953485-CVE-2024-21490-AngularJS-Regular-Expression-Denial-of-Service-ReDoS>
- 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>

Vulnerable Software & Versions (NVD):

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

[CVE-2022-25869](#) suppressed

All versions of package angular 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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:*

[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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406320>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406322>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406321>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos>
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406323>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406325>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406324>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373045>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-resource-trailing-slashes-redos>
- info - <https://github.com/advisories/GHSA-2qqx-w9hr-q5gx>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406326>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406328>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406327>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373046>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos>
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>

Vulnerable Software & Versions (NVD):

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

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://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular.jar

Description:

WebJar for angular

License:

MIT

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/remotegui.zip/angular.jar

MD5: f339a9a66a64c67eebb21ec3b251dfc6

SHA1: cff4aee339a9ca4ae2f095079930edeaad6a94ee

SHA256: a997eb40987ddb5d3bf64adf3d33afc3ac2b1eb2e7255b5203a387f8097cd0

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



CVE-2021-4231 (OSSINDEX) suppressed

A vulnerability was found in Angular up to 11.0.4/11.1.0-next.2. It has been classified as problematic. Affected is the handling of comments. The manipulation leads to cross site scripting. It is possible to launch the attack remotely but it might require an authentication first. Upgrading to version 11.0.5 and 11.1.0-next.3 is able to address this issue. The name of the patch is ba8da742e3b243e8f43d4c63aa842b44e14f2b09. It is recommended to upgrade the affected component.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2021-4231> for details

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 (5.4)
- CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

References:

- OSSINDEX - [\[CVE-2021-4231\] CWE-79: Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4231>
- OSSIndex - <https://github.com/angular/angular/pull/40136>
- OSSIndex - <https://github.com/angular/angular/pull/40525>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.webjars.npm:angular:1.8.3:*:*:*:*:*

CVE-2023-26116 (OSSINDEX) 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

References:

- OSSINDEX - [\[CVE-2023-26116\] CWE-1333](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-26116>
- OSSIndex - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>
- OSSIndex - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos?file=index.js>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.webjars.npm:angular:1.8.3:*:*:*:*:*

CVE-2023-26118 (OSSINDEX) 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.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2023-26118> for details

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

References:

- OSSINDEX - [\[CVE-2023-26118\] CWE-1333](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-26118>
- OSSIndex - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>
- OSSIndex - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos?file=index.js>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.webjars.npm:angular:1.8.3:*:*:*:*:*

remotegui.zip: angular.jar: angular.js

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

MD5: e09f650a016c24bc1b5a1edc93bfade

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

CVSSv2:

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

CVSSv3:

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

References:

- - [FEDORA-2022-e016e6f445](#)
- - [FEDORA-2022-edf635cf39](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220629-0009/>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2772736>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2772738>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2772737>
- MISC - <https://snyk.io/vuln/SNYK-JS-ANGULAR-2772735>
- MISC - <https://stackblitz.com/edit/angularjs-material-blank-zvtdvb>
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:* node.js:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*

[CVE-2024-21490](#) suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- - <https://support.heroku.com/hc/en-us/articles/25715686953485-CVE-2024-21490-AngularJS-Regular-Expression-Denial-of-Service-ReDoS>
- 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>

Vulnerable Software & Versions (NVD):

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

[CVE-2022-25869](#) suppressed

All versions of package angular 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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*

[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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406320>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406322>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406321>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos>
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406323>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406325>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406324>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373045>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-resource-trailing-slashes-redos>
- info - <https://github.com/advisories/GHSA-2qqx-w9hr-q5gx>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406326>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406328>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406327>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373046>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos>
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>

Vulnerable Software & Versions (NVD):

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

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://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

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

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

MD5: 967a32633fa8f38f4ac3376c1a37b992

SHA1: b53b74d8e0b732dcdb98f521146b88299ea2f1

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

CVSSv2:

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

CVSSv3:

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

References:

- - [FEDORA-2022-e016e6f445](#)

- - [FEDORA-2022-edf635cf39](#)
- CONFIRM - <https://security.netapp.com/advisory/ntap-20220629-0009/>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2772736>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2772738>
- MISC - <https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2772737>
- MISC - <https://snyk.io/vuln/SNYK-JS-ANGULAR-2772735>
- MISC - <https://stackblitz.com/edit/angularjs-material-blank-zvtdvb>
- info - <https://github.com/advisories/GHSA-m2h2-264f-f486>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* versions from (including) 1.7.0
- cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:*:*:*:*:*:*

CVE-2024-21490 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746>
- - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747>
- - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113>
- - <https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos>
- - <https://support.heroku.com/hc/en-us/articles/25715686953485-CVE-2024-21490-AngularJS-Regular-Expression-Denial-of-Service-ReDoS>
- 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>

Vulnerable Software & Versions (NVD):

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

CVE-2022-25869 suppressed

All versions of package angular 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

References:

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)

- CONFIRM - [N/A](#)
- CONFIRM - [N/A](#)
- info - <https://github.com/advisories/GHSA-prc3-vjfx-vhm9>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:*

[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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406320>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406322>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406321>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373044>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-angular-copy-redos>
- info - <https://github.com/advisories/GHSA-2vrf-hf26-jrp5>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBRK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406323>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406325>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406324>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373045>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-resource-trailing-slashes-redos>

- info - <https://github.com/advisories/GHSA-2qgx-w9hr-q5gx>

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:angularjs:angular:*:*:*:*:node.js:*:* 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

References:

- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OQWJLE5WE33WNMA54XSJIDXBK2KL3XJ/>
- MISC - <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-5406326>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-5406328>
- MISC - <https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-5406327>
- MISC - <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-3373046>
- MISC - <https://stackblitz.com/edit/angularjs-vulnerability-inpur-url-validation-redos>
- info - <https://github.com/advisories/GHSA-qwqh-hm9m-p5hr>

Vulnerable Software & Versions (NVD):

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

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://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c>
- retid - 54

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: echo2extras-app.jar

Description:

License:

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/remotegui.zip/echo2extras-app.jar

MD5: e1ba37ba20c3021c38e362cac081d986

SHA1: 64e7748149ca2af54ee693c8e232343d64c1b966

SHA256: ad4489475b3c77aeeb62ec1c1bc211c8659b84649fdb1e72f4ee6e005b21e37b

Referenced In Project/Scope: server

Evidence



Related Dependencies



Suppressed Identifiers

- None

Suppressed Vulnerabilities



[CVE-2009-5135](#) suppressed

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

CWE-20 Improper Input Validation

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

CVSSv2:

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

References:

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

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

- [cpe:2.3:a:nextapp:echo:2.1.0:beta5:.*:.*:.*](#)
- ...

remotegui.zip: jquery.jar

Description:

WebJar for jQuery

License:

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/remotegui.zip/jquery.jar

MD5: 4af65e569248d8a2411f66498d720280

SHA1: c3dc40b1b5f24c56afa36fd9a463bb9f378ac4ab

SHA256: de28c4da0ea9f16101352dd3582ec8021ee5e2de5f45104ca171876003d54db6

Referenced In Project/Scope: server

Evidence

Suppressed Identifiers

- None

Suppressed Vulnerabilities

CVE-2019-11358 (OSSINDEX) suppressed

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

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

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

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

CVSSv3:

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

References:

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

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2020-11023 (OSSINDEX) suppressed

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

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

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

CVSSv3:

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

References:

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

Vulnerable Software & Versions (OSSINDEX):

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

remotegui.zip: tinymce.jar: tinymce.js

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/remotegui.zip/tinymce.jar/META-INF/resources/webjars/tinymce/5.10.9/tinymce.js

MD5: f7a8350f10f92d58a952e1feb0d28f2c

SHA1: d3ecc2861e41722d51e1ede38da5ead47a530c14

SHA256: a78ee6bd10002d050a314768a523533144228f654d80571a8ed28ff3011208a1

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



CVE-2024-29203 (RETIREJS) suppressed

Notes: Can not update beyond v5 for implementation reasons just now. tinyMCE is primarily used in non-pulbic way.

Unscored:

- Severity: medium

References:

- info - <https://github.com/advisories/GHSA-438c-3975-5x3f>
- info - <https://github.com/tinymce/tinymce>
- info - <https://github.com/tinymce/tinymce/commit/bcdea2ad14e3c2cea40743fb48c63bba067ae6d1>
- info - <https://github.com/tinymce/tinymce/security/advisories/GHSA-438c-3975-5x3f>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-29203>
- info - https://www.tiny.cloud/docs/tinymce/6/6.8.1-release-notes/#new-convert_unsafe_embeds-option-that-controls-whether-object-and-embed-elements-will-be-converted-to-more-restrictive-alternatives-namely-img-for-image-mime-types-video-for-video-mime-types-audio-audio-mime-types-or-iframe-for-other-or-unspecified-mime-types
- info - https://www.tiny.cloud/docs/tinymce/7/7.0-release-notes/#sandbox_iframes-editor-option-is-now-defaulted-to-true

Vulnerable Software & Versions (RETIREJS):

CVE-2024-29881 (RETIREJS) suppressed

Notes: Can not update beyond v5 for implementation reasons just now. tinyMCE is primarily used in non-pulbic way.

Unscored:

- Severity: medium

References:

- info - <https://github.com/advisories/GHSA-5359-pvf2-pw78>
- info - <https://github.com/tinymce/tinymce>
- info - <https://github.com/tinymce/tinymce/commit/bcdea2ad14e3c2cea40743fb48c63bba067ae6d1>
- info - <https://github.com/tinymce/tinymce/security/advisories/GHSA-5359-pvf2-pw78>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-29881>
- info - https://www.tiny.cloud/docs/tinymce/6/6.8.1-release-notes/#new-convert_unsafe_embeds-option-that-controls-whether-object-and-embed-elements-will-be-converted-to-more-restrictive-alternatives-namely-img-for-image-mime-types-video-for-video-mime-types-audio-audio-mime-types-or-iframe-for-other-or-unspecified-mime-types
- info - https://www.tiny.cloud/docs/tinymce/7/7.0-release-notes/#convert_unsafe_embeds-editor-option-is-now-defaulted-to-true

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: tinymce.jar: tinymce.min.js

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/remotegui.zip/tinymce.jar/META-INF/resources/webjars/tinymce/5.10.9/tinymce.min.js

MD5: 10df005254d5668ccedbdba2614354acd

SHA1: fbcd5a3f14b7c3dd8a9d203b9b30acfba49a38f4

SHA256: 3c3041cb95a1c979ee2205901cf1c670a36c192ef089e6f63b94beabef386c30

Referenced In Project/Scope: server

Evidence



Suppressed Identifiers

- None

Suppressed Vulnerabilities



CVE-2024-29203 (RETIREJS) suppressed

Notes: Can not update beyond v5 for implementation reasons just now. tinyMCE is primarily used in non-pulbic way.

Unscored:

- Severity: medium

References:

- info - <https://github.com/advisories/GHSA-438c-3975-5x3f>
- info - <https://github.com/tinymce/tinymce>
- info - <https://github.com/tinymce/tinymce/commit/bcdea2ad14e3c2cea40743fb48c63bba067ae6d1>
- info - <https://github.com/tinymce/tinymce/security/advisories/GHSA-438c-3975-5x3f>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-29203>
- info - https://www.tiny.cloud/docs/tinymce/6/6.8.1-release-notes/#new-convert_unsafe_embeds-option-that-controls-whether-object-and-embed-elements-will-be-converted-to-more-restrictive-alternatives-namely-img-for-image-mime-types-video-for-video-mime-types-audio-audio-mime-types-or-iframe-for-other-or-unspecified-mime-types
- info - https://www.tiny.cloud/docs/tinymce/7/7.0-release-notes/#sandbox_iframes-editor-option-is-now-defaulted-to-true

Vulnerable Software & Versions (RETIREJS):

CVE-2024-29881 (RETIREJS) suppressed

Notes: Can not update beyond v5 for implementation reasons just now. tinyMCE is primarily used in non-pulbic way.

Unscored:

- Severity: medium

References:

- info - <https://github.com/advisories/GHSA-5359-pvf2-pw78>
- info - <https://github.com/tinymce/tinymce>
- info - <https://github.com/tinymce/tinymce/commit/bcdea2ad14e3c2cea40743fb48c63bba067ae6d1>
- info - <https://github.com/tinymce/tinymce/security/advisories/GHSA-5359-pvf2-pw78>
- info - <https://nvd.nist.gov/vuln/detail/CVE-2024-29881>
- info - https://www.tiny.cloud/docs/tinymce/6/6.8.1-release-notes/#new-convert_unsafe_embeds-option-that-controls-whether-object-and-embed-elements-will-be-converted-to-more-restrictive-alternatives-namely-img-for-image-mime-types-video-for-video-mime-types-audio-audio-mime-types-or-iframe-for-other-or-unspecified-mime-types
- info - https://www.tiny.cloud/docs/tinymce/7/7.0-release-notes/#convert_unsafe_embeds-editor-option-is-now-defaulted-to-true

Vulnerable Software & Versions (RETIREJS):

theme.zip: bootstrap.jar: bootstrap.js

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/theme.zip/bootstrap.jar/META-INF/resources/webjars/bootstrap/3.4.1/js/bootstrap.js

MD5: 894d79839facf38d9fd672bdbe57443d

SHA1: 11277f4e04cf070a350e566b053ef2215993720c

SHA256: dbd2a35e72edc7d6bde483481a912f1c38aa57fab2747d9b071d317339ee03a2
Referenced In Project/Scope: server

Evidence



Related Dependencies



Suppressed Identifiers

- None

Suppressed Vulnerabilities



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

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

Notes: file name: remotegui.zip: bootstrap.jar We are in the process of migrating required functions into a custom framework.

Unscored:

- Severity: low

References:

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

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/reporting/Check-Product-Installer-for-Security-Problems/CRInstaller/server/build/tmp/dependencies/i-net Clear Reports/plugins/theme.zip/bootstrap.jar/META-INF/resources/webjars/bootstrap/3.4.1/js/bootstrap.min.js

MD5: 2f34b630ffe30ba2ff2b91e3f3c322a1

SHA1: b16fd8226bd6bfb08e568f1b1d0a21d60247cefb

SHA256: 9ee2fcff6709e4d0d24b09ca0fc56aade12b4961ed9c43fd13b03248bfb57afe

Referenced In Project/Scope: server

Evidence



Related Dependencies



Suppressed Identifiers

- None

Suppressed Vulnerabilities



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

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

Notes: file name: remotegui.zip: bootstrap.jar We are in the process of migrating required functions into a custom framework.

Unscored:

- Severity: low

References:

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

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](#).