

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

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

Project: root project 'CoWorkInstaller'

cowork:CoWorkInstaller:26.10

Scan Information (show all):

- *dependency-check version*: 13.0.0
- *Report Generated On*: Thu, 15 Oct 2026 17:17:34 +0200
- *Dependencies Scanned*: 1303 (1244 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 129 (show)
- ...

Summary

Summary of Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count

Dependencies (vulnerable)

Suppressed Vulnerabilities

authentication.pam.zip: jna.jar

Description:

JNA Library

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/authentication.pam.zip/jna.jar
MD5: 97fcb12698f8c1e4eed897e5c490e098
SHA1: 50c5b36af5dfd16cab07a1616046a50ec52d1e32
SHA256: 9e5cdb5ff4ad07bf116cb2b37b2b84987041d79a8991766a08b79b085c6bb6c2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Related Dependencies

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2009-2476 suppressed

The Java Management Extensions (JMX) implementation in Sun Java SE 6 before Update 15, and OpenJDK, does not properly enforce OpenType checks, which allows context-dependent attackers to bypass intended access restrictions by leveraging finalizer resurrection to obtain a reference to a privileged object.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513220
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10381
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- secalert@redhat.com - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- secalert@redhat.com - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- secalert@redhat.com - http://secunia.com/advisories/37386
- secalert@redhat.com - http://security.gentoo.org/glsa/glsa-200911-02.xml
- secalert@redhat.com - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- secalert@redhat.com - http://www.vupen.com/english/advisories/2009/2543
- secalert@redhat.com - https://bugzilla.redhat.com/show_bug.cgi?id=513220

- secalert@redhat.com - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10381
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- secalert@redhat.com - PATCH,VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...

CVE-2009-2689 suppressed

JDK13Services.getProviders in Sun Java SE 5.0 before Update 20 and 6 before Update 15, and OpenJDK, grants full privileges to instances of unspecified object types, which allows context-dependent attackers to bypass intended access restrictions via an untrusted (1) applet or (2) application.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

References:
- af854a3a-2127-422b-91ae-364da2661108 - http://java.sun.com/javase/6/webnotes/6u15.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513222
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9603
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY

- cve@mitre.org - http://java.sun.com/javase/6/webnotes/6u15.html
- cve@mitre.org - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/2543
- cve@mitre.org - https://bugzilla.redhat.com/show_bug.cgi?id=513222
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9603
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...

CVE-2009-2475 suppressed

Sun Java SE 5.0 before Update 20 and 6 before Update 15, and OpenJDK, might allow context-dependent attackers to obtain sensitive information via vectors involving static variables that are declared without the final keyword, related to (1) LayoutQueue, (2) Cursor.predefined, (3) AccessibleResourceBundle.getContents, (4) ImageReaderSpi.STANDARD_INPUT_TYPE, (5) ImageWriterSpi.STANDARD_OUTPUT_TYPE, (6) the imageio plugins, (7) DnsContext.debug, (8) RmfFileReader/StandardMidiFileWriter.types, (9) AbstractSaslImpl.logger, (10) Synth.Region.uiToRegionMap/lowerCaseNameMap, (11) the Introspector class and a cache of BeanInfo, and (12) JAX-WS, a different vulnerability than CVE-2009-2673.

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: HIGH (7.8)
- Vector: /AV:N/AC:L/Au:N/C:C/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://java.sun.com/javase/6/webnotes/6u15.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513215

- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10221
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- secalert@redhat.com - http://java.sun.com/javase/6/webnotes/6u15.html
- secalert@redhat.com - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- secalert@redhat.com - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- secalert@redhat.com - http://secunia.com/advisories/37386
- secalert@redhat.com - http://security.gentoo.org/glsa/glsa-200911-02.xml
- secalert@redhat.com - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- secalert@redhat.com - http://www.vupen.com/english/advisories/2009/2543
- secalert@redhat.com - https://bugzilla.redhat.com/show_bug.cgi?id=513215
- secalert@redhat.com - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A10221
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- secalert@redhat.com - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- secalert@redhat.com - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- secalert@redhat.com - PATCH
- secalert@redhat.com - PATCH,VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY
- secalert@redhat.com - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...

CVE-2009-2716 suppressed

The plugin functionality in Sun Java SE 6 before Update 15 does not properly implement version selection, which allows context-dependent attackers to leverage vulnerabilities in "old zip and certificate handling" and have unspecified other impact via unknown vectors.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2676 suppressed

Unspecified vulnerability in JNLPAppletlauncher in Sun Java SE, and SE for Business, in JDK and JRE 6 Update 14 and earlier and JDK and JRE 5.0 Update 19 and earlier; and Java SE for Business in SDK and JRE 1.4.2_21 and earlier; allows remote attackers to create or modify arbitrary files via vectors involving an untrusted Java applet that accesses an old version of JNLPAppletLauncher.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00003.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00002.html
- af854a3a-2127-422b-91ae-364da2661108 - http://marc.info/?l=bugtraq&m=125787273209737&w=2
- af854a3a-2127-422b-91ae-364da2661108 - http://osvdb.org/56789
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.oracle.com/technetwork/topics/security/cpuoct2009-096303.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/bid/35946
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securitytracker.com/id?1022657
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A8453
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - US_GOVERNMENT_RESOURCE

- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-08/msg00003.html
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00002.html
- cve@mitre.org - http://marc.info/?l=bugtraq&m=125787273209737&w=2
- cve@mitre.org - http://osvdb.org/56789
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.oracle.com/technetwork/topics/security/cpuoct2009-096303.html
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.securityfocus.com/bid/35946
- cve@mitre.org - http://www.securitytracker.com/id?1022657
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A8453
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1199.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- cve@mitre.org - PATCH
- cve@mitre.org - PATCH,VENDOR_ADVISORY
- cve@mitre.org - US_GOVERNMENT_RESOURCE
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:*:business:*:*:*:*:*
- ...

CVE-2009-2717 suppressed

The Abstract Window Toolkit (AWT) implementation in Sun Java SE 6 before Update 15 on Windows 2000 Professional does not provide a Security Warning Icon, which makes it easier for context-dependent attackers to trick a user into interacting unsafely with an untrusted applet.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2690 suppressed

The encoder in Sun Java SE 6 before Update 15, and OpenJDK, grants read access to private variables with unspecified names, which allows context-dependent attackers to obtain sensitive information via an untrusted (1) applet or (2) application.

CWE-264 Permissions, Privileges, and Access Controls

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- af854a3a-2127-422b-91ae-364da2661108 - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/2543
- af854a3a-2127-422b-91ae-364da2661108 - https://bugzilla.redhat.com/show_bug.cgi?id=513223
- af854a3a-2127-422b-91ae-364da2661108 - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9443
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- af854a3a-2127-422b-91ae-364da2661108 - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- af854a3a-2127-422b-91ae-364da2661108 - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://lists.apple.com/archives/security-announce/2009/Sep/msg00000.html
- cve@mitre.org - http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00001.html
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.mandriva.com/security/advisories?name=MDVSA-2009:209
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/2543
- cve@mitre.org - https://bugzilla.redhat.com/show_bug.cgi?id=513223
- cve@mitre.org - https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A9443
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1200.html
- cve@mitre.org - https://rhn.redhat.com/errata/RHSA-2009-1201.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00310.html
- cve@mitre.org - https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00325.html
- cve@mitre.org - PATCH
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6
- ...

CVE-2009-2719 suppressed

The Java Web Start implementation in Sun Java SE 6 before Update 15 allows context-dependent attackers to cause a denial of service (NullPointerException) via a crafted .jnlp file, as demonstrated by the jnlp_file/appletDesc/index.html#misc test in the Technology Compatibility Kit (TCK) for the Java Network Launching Protocol (JNLP).

CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

CVE-2009-2720 suppressed

Unspecified vulnerability in the javax.swing.plaf.synth.SynthContext.isSubregion method in the Swing implementation in Sun Java SE 6 before Update 15 allows context-dependent attackers to cause a denial of service (NullPointerException in the Jemmy library) via unknown vectors.

NVD-CWE-noinfo

Notes: file name: authentication.pam.zip: jna.jar False positive match of JNA due to updated NVM matching rules

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37386
- af854a3a-2127-422b-91ae-364da2661108 - http://secunia.com/advisories/37460
- af854a3a-2127-422b-91ae-364da2661108 - http://security.gentoo.org/glsa/glsa-200911-02.xml
- af854a3a-2127-422b-91ae-364da2661108 - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- af854a3a-2127-422b-91ae-364da2661108 - http://www.vmware.com/security/advisories/VMSA-2009-0016.html

- af854a3a-2127-422b-91ae-364da2661108 - http://www.vupen.com/english/advisories/2009/3316
- af854a3a-2127-422b-91ae-364da2661108 - PATCH,VENDOR_ADVISORY
- cve@mitre.org - http://secunia.com/advisories/37386
- cve@mitre.org - http://secunia.com/advisories/37460
- cve@mitre.org - http://security.gentoo.org/glsa/glsa-200911-02.xml
- cve@mitre.org - http://www.securityfocus.com/archive/1/507985/100/0/threaded
- cve@mitre.org - http://www.vmware.com/security/advisories/VMSA-2009-0016.html
- cve@mitre.org - http://www.vupen.com/english/advisories/2009/3316
- cve@mitre.org - PATCH,VENDOR_ADVISORY

Vulnerable Software & Versions:

- cpe:2.3:a:sun:java_se:*:14:*:*:*:*:*:* versions up to (including) 6

cowork.calls.zip: ice4j.jar

Description:

A Java implementation of the ICE protocol

License:

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/ice4j.jar
MD5: eaffb973edafb449ec4e38955f96e267
SHA1: da8ec9b9f069da054184c90129c9cdc9078fc7e9
SHA256: dfce847c62008f044edf0f1448bf9c16b5e80de17a0994289a7581e602075532
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-43550 suppressed

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

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher

but has different version numbers. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is a CVE for a sample phyton project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use. CVE-2026-33117 - azure-core has a different version as the Azure SDK for Java CVE-2026-33117 - we use already jackson 2.22.0 (or higher). The cause can be multiple version ranges in the CVE.

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- support@hackerone.com - PATCH

Vulnerable Software & Versions:

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

cowork.calls.zip: jicoco-config.jar

Description:

Jitsi Common Components (Configuration Utilities)

License:

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jicoco-config.jar
MD5: 2b360a86dbf02f02173b1e4230e19000
SHA1: 0d026d8cf9582bc707641f68ff979da2f60876d6
SHA256: 40295937ec9471edf7bb8d0602b5363c709638033a01505ead4fa99f27b52550
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-43550 suppressed

A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which

could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is a CVE for a sample phyton project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use. CVE-2026-33117 - azure-core has a different version as the Azure SDK for Java CVE-2026-33117 - we use already jackson 2.22.0 (or higher). The cause can be multiple version ranges in the CVE.

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- support@hackerone.com - PATCH

Vulnerable Software & Versions:

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

cowork.calls.zip: jitsi-metaconfig.jar

Description:

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

License:

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jitsi-metaconfig.jar
MD5: f41bbbdb0704a947379e648f92de3b6a
SHA1: 2c324f329f52cf28c14236efe18427e0ce7cf411
SHA256: a5f297490bc6797376e7b814e5c23cd548af5a6d5441bce272f0f1abb07abfe2
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-43550 suppressed

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

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is a CVE for a sample phyton project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use. CVE-2026-33117 - azure-core has a different version as the Azure SDK for Java CVE-2026-33117 - we use already jackson 2.22.0 (or higher). The cause can be multiple version ranges in the CVE.

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- support@hackerone.com - PATCH

Vulnerable Software & Versions:

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

cowork.calls.zip: jitsi-utils.jar

Description:

A set of basic utilities used in Jitsi projects

License:

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/cowork.calls.zip/jitsi-utils.jar
MD5: fa494e8f6b723155f32c3dfb490d8e6e
SHA1: 98b8409c3d8d08aad6a501a32266a669b4252b04
SHA256: aab74933cf6945b99ac3a81d3f27a8753cc3342e97fe522e0b76c18e9ef09923
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-43550 suppressed

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

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection'), CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Notes: false positives, no end date CVE-2008-7271 - This is for the eclipse ide and not for any library from eclipse. CVE-2010-4647 - This is for the eclipse ide and not for any library from eclipse. CVE-2020-26939 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2021-4236 - This is for a go project, match on every lib with 'web' in the name CVE-2021-4277 - This is for a utils project from fredssmith, match on every lib with 'utils' in the name CVE-2022-31548 - This is a CVE for a sample phyton project. CVE-2022-43550 - This is a CVE for the jitsi main project and not for any library from jitsi. CVE-2022-45688 - This is for hutool-json, matched on every component with 'json' in the name CVE-2023-5072 - This is for JSON-java, matched on every component with 'json' in the name CVE-2023-33202 - The BouncyCastle FIPS variant uses same maven package matcher but has different version numbers. CVE-2023-35116 - DISPUTED CVE-2023-36052 - This is for Azure CLI and not for com.azure:azure-core. CVE-2023-45161 - This is for 1E-Exchange which we does not use. CVE-2026-33117 - azure-core has a different version as the Azure SDK for Java CVE-2026-33117 - we use already jackson 2.22.0 (or higher). The cause can be multiple version ranges in the CVE.

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - PATCH
- support@hackerone.com - PATCH

Vulnerable Software & Versions:

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

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/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: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-21490 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: high

References:
- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26116 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2023-26117 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26118 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8372 suppressed

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

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

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8373 suppressed

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

This issue affects all versions of AngularJS.

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

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

Vulnerable Software & Versions (RETIREJS):

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

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

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

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular-animate.jar/META-INF/resources/webjars/angular-animate/1.8.3/angular-animate.min.js
MD5: 5d2d0f42bb7e1b5503e914674f59dad0
SHA1: 4c15a58541e53c451c6f946d2048104f88b833c7
SHA256: 8e6202b1330a469a61ccdeebbd1cb3a20d0ecdfc8d106f68da5b85e9b67a1cd5
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-21490 suppressed

This affects versions of the package angular from 1.3.0; versions of the package angularjs from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in

catastrophic backtracking and cause a denial of service. **Note:**This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26116 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26117 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26118 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8372 suppressed

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

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

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8373 suppressed

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

This issue affects all versions of AngularJS.

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

References:
- ghsaId - GHSA-hfff-63hg-f47j
- info - https://codepen.io/herodevs/pen/RNNEPzP/751b91eab7730dff277523f3d50e4b77
- info - https://github.com/advisories/GHSA-hfff-63hg-f47j

- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2025-4690
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-4690

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: low

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

Vulnerable Software & Versions (RETIREJS):

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

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

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

Unscored:
- Severity: low

References:
- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/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: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-21490 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: high

References:
- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26116 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26117 suppressed

Versions of the package angular from 1.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the $resource service due to the usage of an insecure regular expression.

Exploiting this vulnerability is possible by a large carefully-crafted input, which can result in catastrophic backtracking.

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26118 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-8372 suppressed

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

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

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8373 suppressed

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

This issue affects all versions of AngularJS.

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: low

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

Vulnerable Software & Versions (RETIREJS):

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

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

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

Unscored:
- Severity: low

References:
- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/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: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-21490 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617

- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

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

CVE-2023-26116 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26117 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26118 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8372 suppressed

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

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

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8373 suppressed

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

This issue affects all versions of AngularJS.

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

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

Vulnerable Software & Versions (RETIREJS):

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

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

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

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/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: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-21490 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY

- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: high

References:
- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- report@snyk.io - https://neverendingsupport.github.io/angularjs-poc-cve-2022-25869
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771617
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-6084031
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-2949783

- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBANGULAR-2949784
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2949782
- report@snyk.io - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-2949781

Vulnerable Software & Versions (NVD):

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

CVE-2023-26116 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26117 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26118 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8372 suppressed

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

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

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8373 suppressed

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

This issue affects all versions of AngularJS.

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- 36c7be3b-2937-45df-85ea-ca7133ea542c - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html

- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- info - https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- info - https://www.herodevs.com/vulnerability-directory/cve-2024-8373

Vulnerable Software & Versions (NVD):

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

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: low

References:
- ghsaId - GHSA-j58c-ww9w-pwp5
- info - https://codepen.io/herodevs/pen/qEWQmpd/a86a0d29310e12c7a3756768e6c7b915
- info - https://github.com/advisories/GHSA-j58c-ww9w-pwp5
- info - https://github.com/angular/angular.js

- info - https://nvd.nist.gov/vuln/detail/CVE-2025-0716
- info - https://www.herodevs.com/vulnerability-directory/cve-2025-0716

Vulnerable Software & Versions (RETIREJS):

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

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

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

Unscored:
- Severity: low

References:
- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/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: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-21490 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113

- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: high

References:
- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26116 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26117 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST,THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/UDKFLKJ6VZKL52AFVW2OVZRMJWHMW55K/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2023-26118 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8372 suppressed

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

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

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8373 suppressed

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

This issue affects all versions of AngularJS.

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: low

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

Vulnerable Software & Versions (RETIREJS):

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

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

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

Unscored:
- Severity: low

References:
- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: angular.jar: angular.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/angular.js
MD5: e09f650a016c24bc1b5a1edc93bfbade
SHA1: 0f1f7445b761b9bbd5385f9f0b316dbf1ca48696
SHA256: fdca889e76f55fdee7ab661920f37ce19233563bf7f4ac8120f8ebc2ac768768
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-21490 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: high

References:
- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26116 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26117 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - MAILING_LIST,THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2023-26118 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8372 suppressed

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

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

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8373 suppressed

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

This issue affects all versions of AngularJS.

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: medium

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:
- Severity: low

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

Vulnerable Software & Versions (RETIREJS):

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

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

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

Unscored:

- Severity: low

References:
- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

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

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/angular.jar/META-INF/resources/webjars/angular/1.8.3/angular.min.js
MD5: 967a32633fa8f38f4ac3376c1a37b992
SHA1: b53b74d8e0b732dcdb98fbe521146b88299ea2f1
SHA256: 396dc1a03d6cc02e9c51a80246e0db53c5c8df9bd07287e3b51bce4a29dab355
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2022-25844 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/

- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-m2h2-264f-f486
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/2WUSPYOTOMAZPDEFPWPSCSPMNODRDKK3/
- report@snyk.io - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/7LNAKCNTVBIHWAUT3FKWV5N67PQXSZOO/
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2024-21490 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- HIGH (7.5)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RC:R/MAV:A

References:
- af854a3a-2127-422b-91ae-364da2661108 - https://lists.debian.org/debian-lts-announce/2025/07/msg00005.html
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- info - https://github.com/angular/angular.js
- info - https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- info - https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- info - https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- info - https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos
- report@snyk.io - https://security.snyk.io/vuln/SNYK-DOTNET-ANGULARJS-10771616
- report@snyk.io - EXPLOIT,THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY
- report@snyk.io - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

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

CVE-2026-11998 (RETIREJS) suppressed

Angular's deprecated package has a Cross-Site Scripting issue

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: high

References:

- ghsaId - GHSA-7x27-g8rg-x87w
- info - https://access.redhat.com/security/cve/CVE-2026-11998
- info - https://bugzilla.redhat.com/show_bug.cgi?id=2492579
- info - https://codepen.io/herodevs/pen/JobQdmz/5b3896f56fab66f20cd25e698cf3faa8
- info - https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-11998.json
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998
- info - https://www.herodevs.com/vulnerability-directory/cve-2026-11998?nes-for-angularjs

Vulnerable Software & Versions (RETIREJS):

CVE-2022-25869 suppressed

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26116 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

- MEDIUM (5.3)

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26117 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:

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

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2023-26118 suppressed

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

CWE-1333 Inefficient Regular Expression Complexity

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (5.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8372 suppressed

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

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

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

References:

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

Vulnerable Software & Versions (NVD):

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

CVE-2024-8373 suppressed

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

This issue affects all versions of AngularJS.

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

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

Notes: We can not yet update to newer Angular Version

CVSSv3:
- MEDIUM (4.3)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RC:R/MAV:A

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

Vulnerable Software & Versions (NVD):

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

CVE-2025-2336 (RETIREJS) suppressed

AngularJS Incomplete Filtering of Special Elements vulnerability

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-4690 (RETIREJS) suppressed

AngularJS Regular expression Denial of Service (ReDoS)

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: medium

References:

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

Vulnerable Software & Versions (RETIREJS):

CVE-2025-0716 (RETIREJS) suppressed

AngularJS improperly sanitizes SVG elements

Notes: We can not yet update to newer Angular Version

Unscored:

- Severity: low

References:

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

Vulnerable Software & Versions (RETIREJS):

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

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

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

Unscored:

- Severity: low

References:

- info - https://docs.angularjs.org/misc/version-support-status

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: hugerte.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/hugerte.js
MD5: 608a51d79e72dadae4f71c988978a748
SHA1: f77dd4688fa469741ece9b55f30c07510c83ab1a
SHA256: 9a84cb746a8c0fdd5c857adb90bb4ab0a769335a81246d69224df2decb1bb24b
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2026-66010 suppressed

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

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

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

CVSSv4:
- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:
- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - THIRD_PARTY_ADVISORY
- info - https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197
- info - https://github.com/cure53/DOMPurify/pull/1537
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.12
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4

Vulnerable Software & Versions (NVD):

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

CVE-2026-75838 (RETIREJS) suppressed

DOMPurify: IN_PLACE hook removal leaves a detached subtree executable, causing XSS

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

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-55q2-fjhq-7xh7
- info - https://github.com/cure53/DOMPurify/commit/3067f7746769
- info - https://github.com/cure53/DOMPurify/pull/1557
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.13
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-55q2-fjhq-7xh7

Vulnerable Software & Versions (RETIREJS):

CVE-2026-109345 (RETIREJS) suppressed

DOMPurify: IN_PLACE returns a force-removed rawtext root whose text carries attacker markup — pure HTML reparse executes

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

Unscored:

- Severity: low

References:

- ghsaId - GHSA-6688-9rhm-gjv2
- info - https://github.com/cure53/DOMPurify/commit/b9b9d80f7e401771c2ccaef5f45def7eec8f27d7
- info - https://github.com/cure53/DOMPurify/pull/1636
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.16
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-6688-9rhm-gjv2

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: hugerte.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/hugerte.min.js
MD5: 4f869562fbf4bb6f160fb4bf6ec6599f
SHA1: a86e8883ad71949b770498c57966f60ea42518f7
SHA256: be8e43ec41c91e98897e19594c67eeb98fbe269a67cdab2cfb8cb79d298ff05c
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2026-66010 suppressed

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

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

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

CVSSv4:
- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:
- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - THIRD_PARTY_ADVISORY
- info - https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197
- info - https://github.com/cure53/DOMPurify/pull/1537
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.12
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4

Vulnerable Software & Versions (NVD):

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

CVE-2026-75838 (RETIREJS) suppressed

DOMPurify: IN_PLACE hook removal leaves a detached subtree executable, causing XSS

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

Unscored:
- Severity: medium

References:
- ghsaId - GHSA-55q2-fjhq-7xh7
- info - https://github.com/cure53/DOMPurify/commit/3067f7746769
- info - https://github.com/cure53/DOMPurify/pull/1557
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.13
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-55q2-fjhq-7xh7

Vulnerable Software & Versions (RETIREJS):

CVE-2026-109345 (RETIREJS) suppressed

DOMPurify: IN_PLACE returns a force-removed rawtext root whose text carries attacker markup — pure HTML reparse executes

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

Unscored:
- Severity: low

References:
- ghsaId - GHSA-6688-9rhm-gjv2
- info - https://github.com/cure53/DOMPurify/commit/b9b9d80f7e401771c2ccaef5f45def7eec8f27d7

- info - https://github.com/cure53/DOMPurify/pull/1636
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.16
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-6688-9rhm-gjv2

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: theme.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/themes/silver/theme.js
MD5: cf817d8941a3c0111193ece2d7c9b929
SHA1: f7a71244e44dcbf90a9804051bd788b293289a8e
SHA256: 8e0f595de763e6ede53566f5516c6744a175fabd46c40ba3cba6ed39140bb926
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2026-66010 suppressed

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

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

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

CVSSv4:
- MEDIUM (5.1)
- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSSv3:
- MEDIUM (6.1)
- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RC:R/MAV:A

References:
- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - THIRD_PARTY_ADVISORY
- info - https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197
- info - https://github.com/cure53/DOMPurify/pull/1537
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.12
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4

Vulnerable Software & Versions (NVD):

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

CVE-2026-75838 (RETIREJS) suppressed

DOMPurify: IN_PLACE hook removal leaves a detached subtree executable, causing XSS

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

Unscored:
- Severity: medium

References:
- ghsaId - GHSA-55q2-fjhq-7xh7
- info - https://github.com/cure53/DOMPurify/commit/3067f7746769
- info - https://github.com/cure53/DOMPurify/pull/1557
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.13
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-55q2-fjhq-7xh7

Vulnerable Software & Versions (RETIREJS):

CVE-2026-109345 (RETIREJS) suppressed

DOMPurify: IN_PLACE returns a force-removed rawtext root whose text carries attacker markup — pure HTML reparse executes

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

Unscored:
- Severity: low

References:
- ghsaId - GHSA-6688-9rhm-gjv2
- info - https://github.com/cure53/DOMPurify/commit/b9b9d80f7e401771c2ccaef5f45def7eec8f27d7
- info - https://github.com/cure53/DOMPurify/pull/1636
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.16
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-6688-9rhm-gjv2

Vulnerable Software & Versions (RETIREJS):

remotegui.zip: hugerte.jar: theme.min.js

File Path: /home/jenkins/workspace/cowork/Check-Product-Installer-for-Security-Problems/CoWorkInstaller/build/tmp/dependencies/i-net CoWork/plugins/remotegui.zip/hugerte.jar/META-INF/resources/webjars/hugerte/1.0.12/themes/silver/theme.min.js
MD5: 8bf8c393660a3656dc0e4b9f12bdc697
SHA1: 49a25ecc5db9c1e0f63804f3ab89885d7d0119f9
SHA256: a43e3e8ec4abb5adff7d91c3c7fe12323920c7bccbcd47ba84625353a012d513
Referenced In Project/Scope: CoWorkInstaller

Evidence

Suppressed Identifiers

- **None**

Suppressed Vulnerabilities

CVE-2026-66010 suppressed

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

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

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

CVSSv4:

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

CVSSv3:

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

References:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - EXPLOIT,VENDOR_ADVISORY
- disclosure@vulncheck.com - THIRD_PARTY_ADVISORY
- info - https://github.com/cure53/DOMPurify/commit/a9ca1e537422319a557a9a2aa61f003b23b4a197
- info - https://github.com/cure53/DOMPurify/pull/1537
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.12
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-c2j3-45gr-mqc4

Vulnerable Software & Versions (NVD):

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

CVE-2026-75838 (RETIREJS) suppressed

DOMPurify: IN_PLACE hook removal leaves a detached subtree executable, causing XSS

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

Unscored:

- Severity: medium

References:

- ghsaId - GHSA-55q2-fjhq-7xh7
- info - https://github.com/cure53/DOMPurify/commit/3067f7746769
- info - https://github.com/cure53/DOMPurify/pull/1557
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.13
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-55q2-fjhq-7xh7

Vulnerable Software & Versions (RETIREJS):

CVE-2026-109345 (RETIREJS) suppressed

DOMPurify: IN_PLACE returns a force-removed rawtext root whose text carries attacker markup — pure HTML reparse executes

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

Unscored:

- Severity: low

References:

- ghsaId - GHSA-6688-9rhm-gjv2
- info - https://github.com/cure53/DOMPurify/commit/b9b9d80f7e401771c2ccaef5f45def7eec8f27d7
- info - https://github.com/cure53/DOMPurify/pull/1636
- info - https://github.com/cure53/DOMPurify/releases/tag/3.4.16
- info - https://github.com/cure53/DOMPurify/security/advisories/GHSA-6688-9rhm-gjv2

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 Guide OSS Index API.