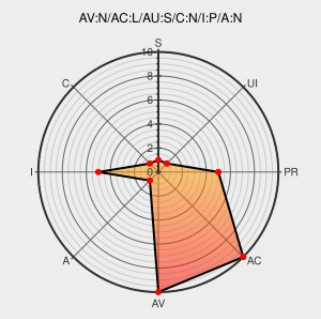
CVE-2015-5253

Published on: 11/18/2015 12:00:00 AM UTC

Last Modified on: 06/16/2021 12:15:00 PM UTC

CVE-2015-5253

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cxf from Apache contain the following vulnerability:

The SAML Web SSO module in Apache CXF before 2.7.18, 3.0.x before 3.0.7, and 3.1.x before 3.1.3 allows remote authenticated users to bypass authentication via a crafted SAML response with a valid signed assertion, related to a "wrapping attack."

CVE-2015-5253 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Apache CXF SAML SSO Module Lets Remote Users Conduct XML Wrapping Attacks to Bypass Authentication on the Target System - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1034162
Pony Mail!	lists.apache.org, text/html	MLIST [cxf-commits] 20200116 svn commit: r1055336 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2019-12423.txt.asc security-advisories.data/CVE-2019-17573.txt.asc security-advisories.html
Red Hat Customer Portal	Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2016:0321
	Vendor Advisory	CONFIRM cxf.apache.org/security-advisories.data/CVE-2015-

	cxf.apache.org text/plain	5253.txt.asc
Pony Mail!	lists.apache.org text/html	MLIST [cxf-commits] 20210402 svn commit: r1073270 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2021-22696.txt.asc security-advisories.html
Pony Mail!	lists.apache.org text/html	MLIST [cxf-commits] 20200319 svn commit: r1058035 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2019-17573.txt.asc security-advisories.html
oss-security - New security advisory for Apache CXF	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20151114 New security advisory for Apache CXF
Pony Mail!	lists.apache.org text/html	MLIST [cxf-commits] 20200401 svn commit: r1058573 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.data/CVE-2020-1954.txt.asc security-advisories.html
ASF Git Repos - cxf.git/commitdiff	Vendor Advisory git-wip-us.apache.org text/xml	CONFIRM git-wip-us.apache.org/repos/asf?p=cxf.git;a=commitdiff;h=845eccb6484b43ba02875c71e824db23ae4f20c0
Pony Mail!	lists.apache.org text/html	MLIST [cxf-commits] 20210616 svn commit: r1075801 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.data/CVE-2021-30468.txt.asc security-advisories.html
Pony Mail!	lists.apache.org text/html	MLIST [cxf-commits] 20201112 svn commit: r1067927 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2020-13954.txt.asc security-advisories.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Cxf	All	All	All	All
Application	Apache	Cxf	All	All	All	All

cpe:2.3:a:apache:cxf:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:cxf:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report