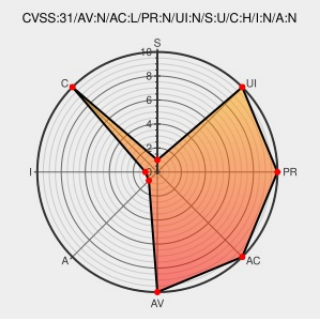
CVE-2021-40690

Published on: 09/19/2021 12:00:00 AM UTC

Last Modified on: 12/03/2021 02:50:00 AM UTC

CVE-2021-40690

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Cxf from Apache contain the following vulnerability:

All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.

CVE-2021-40690 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache Santuario** version **< 2.2.3,2.1.7**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	MLIST [tomee-commits] 20210923 [jira] [Updated] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-202

Debian -- Security Information -- DSA-5010-1 libxml-security-java	www.debian.org Depreciated Link text/html	DEBIAN DSA-5010
Pony Mail!	lists.apache.org text/html	MLIST [tomee-commits] 20211028 [jira] [Updated] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-202
[SECURITY] [DLA 2767-1] libxml-security-java security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20210927 [SECURITY] [DLA 2767-1] libxml-security-java security update
Pony Mail!	lists.apache.org text/html	MLIST [tomee-commits] 20210922 [tomee] 02/02: Update xmlsec to 2.2.3 to mitigate CVE-2021-40690
Pony Mail!	lists.apache.org text/html	MISC lists.apache.org/thread.html/r8848751b6a5dd78cc9e99d627e74fecfaffdfa1bb615dce827aad633%40%3Cde
Pony Mail!	lists.apache.org text/html	MLIST [poi-user] 20210923 Re: CVE-2021-40690 on xmlsec jar
Pony Mail!	lists.apache.org text/html	MLIST [tomee-commits] 20210923 [jira] [Resolved] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-20
Pony Mail!	lists.apache.org text/html	MLIST [tomee-commits] 20210923 [jira] [Created] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-202
Pony Mail!	lists.apache.org text/html	MLIST [cxf-issues] 20211027 [jira] [Created] (CXF-8613) High Security issues reported with Apache San CXF 3.4.4
Pony Mail!	lists.apache.org text/html	MLIST [tomee-commits] 20210923 [jira] [Assigned] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-20

Related QID Numbers

178811 Debian Security Update for libxml-security-java (DLA 2767-1)

178899 Debian Security Update for libxml-security-java (DSA 5010-1)

239965 Red Hat Update for JBoss Enterprise Application Platform 7.3.10 on RHEL 7 (RHSA-2021:5150)

239966 Red Hat Update for JBoss Enterprise Application Platform 7.3.10 on RHEL 8 (RHSA-2021:5151)

239967 Red Hat Update for JBoss Enterprise Application Platform 7.3.10 on RHEL 6 (RHSA-2021:5149)

980105 Java (maven) Security Update for org.apache.santuario:xmlsec (GHSA-j8wc-gxx9-82hx)

Exploit/POC from Github

PoC for exploiting CVE-2021-40690 : All versions of Apache Santuario - XML Security for

Java prior to 2.2.3 and 2.1.7…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Cxf	3.4.4	All	All	All
Application	Apache	Tomee	All	All	All	All
Application	Apache	Xml Security For Java	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

cpe:2.3:a:apache:cxf:3.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:apache:tomee:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:xml_security_for_java:*:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

Discovery Credit

An Trinh, Calif.

Social Mentions

Source	Title	Posted (UTC)
@oss_security	CVE-2021-40690: Apache Santuario: Bypass of the secureValidation property: Posted by Colm O hEigeartaigh on Sep 17D… twitter.com/i/web/status/1…	2021-09-17 13:14:02
@CVEreport	CVE-2021-40690 : All versions of #Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable… twitter.com/i/web/status/1…	2021-09-19 17:27:43
@0_exploit	CVE-2021-40690 dlvr.it/S7tQ8W	2021-09-19 22:53:01

← Previous ID

Next ID→

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