



# CVE-2021-40690

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

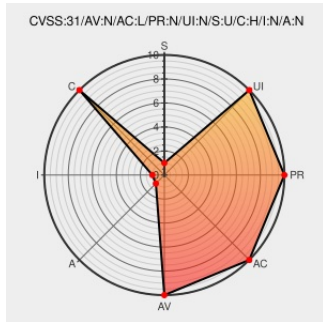
Last Modified on: 12/03/2021 02:50:00 AM UTC

## 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
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>NONE</b>	<b>NONE</b>

CVSS2 Score: **5 - MEDIUM**


Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>NONE</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Pony Mail!	<a href="#">lists.apache.org</a> <a href="#">text/html</a>	<a href="#">MLIST [tomee-commits] 20210923 [jira] [Updated] (TOME-3798) TomEE (8.0.8) is affected by CVE-2021-40690</a>


Debian -- [www.debian.org](http://www.debian.org)  DEBIAN DSA-5010  
Security [Deprecated Link](#)  
Information [text/html](#)  
-- DSA-  
5010-1  
libxml-  
security-  
java

Pony Mail! [lists.apache.org](http://lists.apache.org)  MLIST [tomee-commits] 20211028 [jira] [Updated] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-2021-40690 [text/html](#)


[SECURITY] [lists.debian.org](http://lists.debian.org)  MLIST [debian-lts-announce] 20210927 [SECURITY] [DLA 2767-1] libxml-security-java security update  
[DLA 2767-  
1] libxml-  
security-  
java security  
update


Pony Mail! [lists.apache.org](http://lists.apache.org)  MLIST [tomee-commits] 20210922 [tomee] 02/02: Update xmlsec to 2.2.3 to mitigate CVE-2021-40690 [text/html](#)

Pony Mail! [lists.apache.org](http://lists.apache.org)  MISC  
[lists.apache.org/thread.html/r8848751b6a5dd78cc9e99d627e74fecfaaffda1bb615dce827aad633%40%3Cde](http://lists.apache.org/thread.html/r8848751b6a5dd78cc9e99d627e74fecfaaffda1bb615dce827aad633%40%3Cde)

Pony Mail! [lists.apache.org](http://lists.apache.org)  MLIST [poi-user] 20210923 Re: CVE-2021-40690 on xmlsec jar [text/html](#)

Pony Mail! [lists.apache.org](http://lists.apache.org)  MLIST [tomee-commits] 20210923 [jira] [Resolved] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-2021-40690 [text/html](#)

Pony Mail! [lists.apache.org](http://lists.apache.org)  MLIST [tomee-commits] 20210923 [jira] [Created] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-2021-40690 [text/html](#)

Pony Mail! [lists.apache.org](http://lists.apache.org)  MLIST [cxf-issues] 20211027 [jira] [Created] (CXF-8613) High Security issues reported with Apache Santuario CXF 3.4.4 [text/html](#)

Pony Mail! [lists.apache.org](http://lists.apache.org)  MLIST [tomee-commits] 20210923 [jira] [Assigned] (TOMEE-3798) TomEE (8.0.8) is affected by CVE-2021-40690 [text/html](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

## 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	<a href="#">Apache</a>	<a href="#">Cxf</a>	3.4.4	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomee</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Xml Security For Java</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-09-19 17:27:43
 @0_exploit	CVE-2021-40690 <a href="https://dlvr.it/S7tQ8W">dlvr.it/S7tQ8W</a>	2021-09-19 22:53:01

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**