



CVE-2017-5653

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-5653
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-18 16:59:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	JAX-RS XML Security streaming clients in Apache CXF before 3.1.11 and 3.0.13 do not validate that the service response

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
[cxf-commits] 20210402 svn commit: r1073270 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-2017-5653.txt.asc
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
cxf.apache.org/security-advisories.data/CVE-2017-5653.txt.asc
Pony Mail!
[cxf-commits] 20210616 svn commit: r1075801 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.data/CVE-2017-5653.txt.asc
Apache CXF CVE-2017-5653 Spoofing Vulnerability
Pony Mail!
Pony Mail!

Pony Mail!
Pony Mail!
Apache CXF JAX-RS XML Security Streaming Client Validation Flaw Lets Remote Users Bypass Security Restrictions on the Target System -
Pony Mail!
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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