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-20
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.da
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.