CVE-2017-5656

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-5656
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	Apache CXF's STSClient before 3.1.11 and 3.0.13 uses a flawed way of caching tokens that are associated with delegation

Risk And Classification

Problem Types: CWE-384

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
Apache CXF CVE-2017-5656 Information Disclosure Vulnerability
[cxf-commits] 20210402 svn commit: r1073270 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-20
Pony Mail!
Apache CXF STSClient Token Caching Bug Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker
Pony Mail!
cxf.apache.org/security-advisories.data/CVE-2017-5656.txt.asc
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
[cxf-commits] 20210616 svn commit: r1075801 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.da
Pony Mail!

Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
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.