



CVE-2017-12631

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

Summary

CVE	CVE-2017-12631
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-30 14:29:00 UTC
Updated	2023-11-07 02:38:00 UTC
Description	Apache CXF Fediz ships with a number of container-specific plugins to enable WS-Federation for applications. A CSRF (Cr

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Cxf Fediz	All	All	All	All
Application	Apache	Cxf Fediz	1.4.0	All	All	All
Application	Apache	Cxf Fediz	1.4.1	All	All	All
Application	Apache	Cxf Fediz	1.4.2	All	All	All
Application	Apache	Cxf Fediz	All	All	All	All
Application	Apache	Cxf Fediz	1.4.0	All	All	All
Application	Apache	Cxf Fediz	1.4.1	All	All	All
Application	Apache	Cxf Fediz	1.4.2	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!
Apache CXF Fediz Access Control Flaw in Spring Plugins Lets Remote Users Conduct Cross-Site Request Forgery Attacks - SecurityTracker
Pony Mail!
Pony Mail!
Pony Mail!

Apache CXF Fediz CVE-2017-12631 Multiple Cross Site Request Forgery Vulnerabilities
Pony Mail!
[cxf-commits] 20210616 svn commit: r1075801 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.da
cxf-user - Apache CXF Fediz 1.4.3 and 1.3.3 released with a new security advisory CVE-2017-12631
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
Legacy QID Mappings
982222 Java (maven) Security Update for org.apache.cxf.fediz:fediz-spring (GHSA-fv7x-4hpc-hf9f)

© [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](#)