



CVE-2017-5657

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2017-5657 |
| State | PUBLIC |
| Assigner | security@apache.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-05-22 18:29:00 UTC |
| Updated | 2023-11-07 02:49:00 UTC |
| Description | Several REST service endpoints of Apache Archiva are not protected against Cross Site Request Forgery (CSRF) attacks. |

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Apache | Archiva | All | All | All | All |

References

Reference

Pony Mail!

Pony Mail!

Apache Archiva Access Control Flaw at Several REST Endpoints Lets Remote Users Conduct Cross-Site Request Forgery Attacks - Security

Archiva – Security Vulnerabilities

Apache Archiva CVE-2017-5657 Multiple Cross-Site Request Forgery Vulnerabilities

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](#).

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