



CVE-2016-5000

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

Summary

CVE	CVE-2016-5000
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-05 14:59:00 UTC
Updated	2023-11-07 02:32:00 UTC
Description	The XLSX2CSV example in Apache POI before 3.14 allows remote attackers to read arbitrary files via a crafted OpenXML c

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- Apache POI CVE-2016-5000 XML External Entity Injection Vulnerability
- Pony Mail!
- Pony Mail!
- Oracle Critical Patch Update Advisory - October 2020
- SecurityFocus
- IBM InfoSphere Information Server XML External Entity Processing Flaw in Apache POI Lets Remote Users Obtain Potentially Sensitive Inform
- Security Bulletin: Vulnerabilities in Apache POI affects IBM InfoSphere Information Server
- 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](#)