CVE-2017-1156

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

Summary

CVE	CVE-2017-1156
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-05 19:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	IBM WebSphere Portal 8.5 and 9.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Websphere Portal	8.5	All	All	All
Application	Ibm	Websphere Portal	9.0	All	All	All
Application	Ibm	Websphere Portal	8.5	All	All	All
Application	Ibm	Websphere Portal	9.0	All	All	All

References

Reference	S
IBM notice: The page you requested cannot be displayed	C
IBM WebSphere Portal CVE-2017-1156 Unspecified Open Redirection Vulnerability	B
IBM WebSphere Portal Open Redirect Flaw Lets Remote Users Redirect the Target User's Browser to an Arbitrary Site - SecurityTracker	S
CVE Program record	C
NVD vulnerability detail	N

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 registred 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