



CVE-2011-2487

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

Summary

CVE	CVE-2011-2487
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-11 16:15:00 UTC
Updated	2023-02-13 01:19:00 UTC
Description	The implementations of PKCS#1 v1.5 key transport mechanism for XMLEncryption in JBossWS and Apache WSS4J before

Risk And Classification

Problem Types: CWE-327

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
Application	Apache	Wss4j	All	All	All	All
Application	Apache	Wss4j	All	All	All	All
Application	Redhat	JBoss Business Rules Management System	5.3	All	All	All
Application	Redhat	JBoss Business Rules Management System	5.3	All	All	All
Application	Redhat	JBoss Enterprise Application Platform	5.0.0	All	All	All
Application	Redhat	JBoss Enterprise Application Platform	5.0.0	All	All	All
Application	Redhat	JBoss Enterprise Application Platform Text-only Advisories	-	All	All	All
Application	Redhat	JBoss Enterprise Application Platform Text-only Advisories	-	All	All	All
Application	Redhat	JBoss Enterprise Soa Platform	4.2.0	All	All	All
Application	Redhat	JBoss Enterprise Soa Platform	4.3.0	All	All	All
Application	Redhat	JBoss Enterprise Soa Platform	4.2.0	All	All	All
Application	Redhat	JBoss Enterprise Soa Platform	4.3.0	All	All	All
Application	Redhat	JBoss Enterprise Web Platform	5.0.0	All	All	All
Application	Redhat	JBoss Enterprise Web Platform	5.0.0	All	All	All
Application	Redhat	JBoss Middleware Text-only Advisories	-	All	All	All

Application	Redhat	Jboss Middleware Text-only Advisories	-	All	All	All
Application	Redhat	Jboss Portal	4.0.0	All	All	All
Application	Redhat	Jboss Portal	4.0.0	All	All	All
Application	Redhat	Jboss Web Services	-	All	All	All
Application	Redhat	Jboss Web Services	-	All	All	All

References

Reference	Source
Red Hat Customer Portal	MISC
Red Hat Customer Portal	MISC
CVE-2011-2487 - Red Hat Customer Portal	MISC
Veröffentlichungen - Ruhr-Universität Bochum	MISC
Pony Mail!	MLIST
Pony Mail!	MLIST
Red Hat Customer Portal	MISC
Red Hat Customer Portal	MISC
Red Hat Customer Portal	MISC
Pony Mail!	MISC
Red Hat Customer Portal	MISC
lists.apache.org/thread.html/rec7160382badd3ef4ad017a22f64a266c7188b9ba71394f0...	MISC
Red Hat Customer Portal	MISC
Red Hat Customer Portal	MISC
lists.apache.org/thread.html/rfb87e0bf3995e7d560afeed750fac9329ff5f1ad49da3651...	MISC
JBoss Enterprise Application Platform CVE-2011-2487 Information Disclosure Vulnerability	MISC
Red Hat Customer Portal	MISC
Pony Mail!	MLIST
Red Hat Customer Portal	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Pony Mail!	MLIST
Pony Mail!	MLIST
Red Hat Customer Portal	MISC
Red Hat Customer Portal	MISC
Apache CXF -- Note on CVE-2011-2487	MISC
Red Hat Customer Portal	MISC

Red Hat Customer Portal	MISC
Pony Mail!	MISC
Red Hat Customer Portal	MISC
Pony Mail!	MISC
Red Hat Customer Portal	MISC
Red Hat Customer Portal	MISC
713539 – (CVE-2011-2487) CVE-2011-2487 jbossws: Prone to Bleichenbacher attack against to be distributed symmetric key	MISC
IBM X-Force Exchange	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)