



CVE-2012-2312

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2012-2312
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-18 18:15:00 UTC
Updated	2019-12-23 20:32:00 UTC
Description	An Elevated Privileges issue exists in JBoss AS 7 Community Release due to the improper implementation in the security c

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Application Server	7.1.0	All	All	All
Application	Redhat	Jboss Application Server	7.1.1	All	All	All
Application	Redhat	Jboss Application Server	7.1.0	All	All	All
Application	Redhat	Jboss Application Server	7.1.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	beta	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	beta	All	All

References

Reference

CVE-2012-2312

CVE-2012-2312 - Red Hat Customer Portal

Bug 818837 – CVE-2012-2312 JBoss AS 7: Security Context Propagation - When re-using thread from thread pool, security context also gets

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](#).

Free CVE JSON API [cve.report/api](#)

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