CVE-2015-3198

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

Summary

CVE	CVE-2015-3198
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-21 14:29:00 UTC
Updated	2017-08-07 16:43:00 UTC
Description	The Undertow module of WildFly 9.x before 9.0.0.CR2 and 10.x before 10.0.0.Alpha1 allows remote attackers to obtain the

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Wildfly Application Server	9.0.0	beta1	All	All
Application	Redhat	Jboss Wildfly Application Server	9.0.0	beta2	All	All
Application	Redhat	Jboss Wildfly Application Server	9.0.0	cr1	All	All
Application	Redhat	Jboss Wildfly Application Server	9.0.0	beta1	All	All
Application	Redhat	Jboss Wildfly Application Server	9.0.0	beta2	All	All
Application	Redhat	Jboss Wildfly Application Server	9.0.0	cr1	All	All

References

Reference	Source	Link
[WFLY-4595] JSP source code leak when a slash added at the end of the URL - JBoss Issue Tracker	CONFIRM	issues
With trailing slash in URL , jsp show source code |JBoss Developer	MISC	develo
1224787 – (CVE-2015-3198) CVE-2015-3198 JBOSS: JSP source code leak when a slash added at the end of the URL	CONFIRM	bugzil
wildfly - With trailing slash in URL , jsp show source code - Stack Overflow	MISC	stacko
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**