



# CVE-2019-14838

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

## Summary

<b>CVE</b>	CVE-2019-14838
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-10-14 15:15:00 UTC
<b>Updated</b>	2020-10-13 16:21:00 UTC
<b>Description</b>	A flaw was found in wildfly-core before 7.2.5.GA. The Management users with Monitor, Auditor and Deployer Roles should

## Risk And Classification

**Problem Types:** CWE-269

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Data Grid	7.3.4	All	All	All
Application	Redhat	Data Grid	7.3.4	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.4	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.5	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.4	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.2.5	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.3.0	All	All	All
Application	Redhat	Single Sign-on	7.3.5	All	All	All

Application	Redhat	Single Sign-on	7.3.5	All	All	All
Application	Redhat	Wildfly Core	7.0.0	-	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha1	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha2	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha3	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha4	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha5	All	All
Application	Redhat	Wildfly Core	7.0.0	beta1	All	All
Application	Redhat	Wildfly Core	7.0.0	cr1	All	All
Application	Redhat	Wildfly Core	7.0.0	-	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha1	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha2	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha3	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha4	All	All
Application	Redhat	Wildfly Core	7.0.0	alpha5	All	All
Application	Redhat	Wildfly Core	7.0.0	beta1	All	All
Application	Redhat	Wildfly Core	7.0.0	cr1	All	All

## References

Reference	Source
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
1751227 – (CVE-2019-14838) CVE-2019-14838 wildfly-core: Incorrect privileges for 'Monitor', 'Auditor' and 'Deployer' user by default	CONF
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
Red Hat Customer Portal	REDH
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[994589](#) Java (Maven) Security Update for org.wildfly.core:wildfly-core-parent (GHSA-82v2-f875-73g9)

© [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](#)