



CVE-2017-15089

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

Summary

CVE	CVE-2017-15089
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-15 17:29:00 UTC
Updated	2019-06-04 17:29:00 UTC
Description	It was found that the Hotrod client in Infinispan before 9.2.0.CR1 would unsafely read deserialized data on information from

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Infinispan	Infinispan	9.2.0	alpha1	All	All
Application	Infinispan	Infinispan	9.2.0	alpha2	All	All
Application	Infinispan	Infinispan	9.2.0	beta1	All	All
Application	Infinispan	Infinispan	9.2.0	beta2	All	All
Application	Infinispan	Infinispan	9.2.0	cr1	All	All
Application	Infinispan	Infinispan	9.2.0	alpha1	All	All
Application	Infinispan	Infinispan	9.2.0	alpha2	All	All
Application	Infinispan	Infinispan	9.2.0	beta1	All	All
Application	Infinispan	Infinispan	9.2.0	beta2	All	All
Application	Infinispan	Infinispan	9.2.0	cr1	All	All
Application	Infinispan	Infinispan	All	All	All	All

References

Reference
Red Hat Customer Portal
Red Hat Customer Portal
ISPN-8624 Extend unmarshalling white list to GenericJBossMarshaller by galderz · Pull Request #5639 · infinispan/infinispan · GitHub

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat JBoss Data Grid Deserialization Flaw in Infinispan Lets Remote Authenticated Users Execute Arbitrary Code on the Target System -

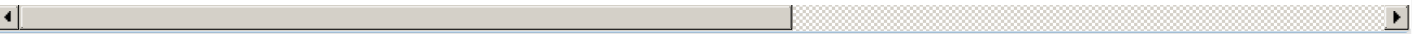
Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

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](#).

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