



CVE-2017-7525

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

Summary

CVE	CVE-2017-7525
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-06 15:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	A deserialization flaw was discovered in the jackson-databind, versions before 2.6.7.1, 2.7.9.1 and 2.8.9, which could allow

Risk And Classification

Problem Types: CWE-184

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Struts	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Fasterxml	Jackson-databind	All	All	All	All
Application	Fasterxml	Jackson-databind	2.9.0	prerelease1	All	All
Application	Fasterxml	Jackson-databind	2.9.0	prerelease2	All	All
Application	Fasterxml	Jackson-databind	All	All	All	All
Application	Fasterxml	Jackson-databind	2.9.0	prerelease1	All	All
Application	Fasterxml	Jackson-databind	2.9.0	prerelease2	All	All
Application	Netapp	Oncommand Balance	-	All	All	All
Application	Netapp	Oncommand Balance	-	All	All	All
Application	Netapp	Oncommand Performance Manager	-	All	All	All
Application	Netapp	Oncommand Performance Manager	-	All	All	All
Application	Netapp	Oncommand Performance Manager	-	All	All	All
Application	Netapp	Oncommand Performance Manager	-	All	All	All

Application	Netapp	Oncommand Shift	-	All	All	All
Application	Netapp	Oncommand Shift	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Oracle	Banking Platform	2.5.0	All	All	All
Application	Oracle	Banking Platform	2.6.0	All	All	All
Application	Oracle	Banking Platform	2.6.1	All	All	All
Application	Oracle	Banking Platform	2.6.2	All	All	All
Application	Oracle	Banking Platform	2.5.0	All	All	All
Application	Oracle	Banking Platform	2.6.0	All	All	All
Application	Oracle	Banking Platform	2.6.1	All	All	All
Application	Oracle	Banking Platform	2.6.2	All	All	All
Application	Oracle	Communications Billing And Revenue Management	12.0	All	All	All
Application	Oracle	Communications Billing And Revenue Management	7.5	All	All	All
Application	Oracle	Communications Billing And Revenue Management	12.0	All	All	All
Application	Oracle	Communications Billing And Revenue Management	7.5	All	All	All
Application	Oracle	Communications Communications Policy Management	All	All	All	All
Application	Oracle	Communications Diameter Signaling Route	All	All	All	All
Application	Oracle	Communications Diameter Signaling Route	All	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1.2.0	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1.2.0	All	All	All
Application	Oracle	Enterprise Manager For Virtualization	13.2.2	All	All	All
Application	Oracle	Enterprise Manager For Virtualization	13.2.3	All	All	All
Application	Oracle	Enterprise Manager For Virtualization	13.3.1	All	All	All
Application	Oracle	Enterprise Manager For Virtualization	13.2.2	All	All	All
Application	Oracle	Enterprise Manager For Virtualization	13.2.3	All	All	All
Application	Oracle	Enterprise Manager For Virtualization	13.3.1	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.2.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.3.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.4.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.5.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.6.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.7.0.0	All	All	All

Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.2.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.3.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.4.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.5.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.6.0.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	8.0.7.0.0	All	All	All
Application	Oracle	Global Lifecycle Management Opatchauto	All	All	All	All
Application	Oracle	Global Lifecycle Management Opatchauto	All	All	All	All
Application	Oracle	Primavera Unifier	16.1	All	All	All
Application	Oracle	Primavera Unifier	16.2	All	All	All
Application	Oracle	Primavera Unifier	18.8	All	All	All
Application	Oracle	Primavera Unifier	16.1	All	All	All
Application	Oracle	Primavera Unifier	16.2	All	All	All
Application	Oracle	Primavera Unifier	18.8	All	All	All
Application	Oracle	Primavera Unifier	All	All	All	All
Application	Oracle	Utilities Advanced Spatial And Operational Analytics	2.7.0.1	All	All	All
Application	Oracle	Utilities Advanced Spatial And Operational Analytics	2.7.0.1	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.3.0	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.3.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.1	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All

Application	Hedhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

Document Display | HPE Support Center

Pony Mail!

[SECURITY] [DLA 2091-1] libjackson-json-java security update

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

Jackson Deserializer security vulnerability via default typing · Issue #1599 · FasterXML/jackson-databind · GitHub

S2-055 - Apache Struts 2 Documentation - Apache Software Foundation

Red Hat Customer Portal

Pony Mail!

Deserialization vulnerability via polymorphic deserialization (CVE-2017-7525) · Issue #1723 · FasterXML/jackson-databind · GitHub

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

CPU July 2018

Oracle Critical Patch Update - April 2018

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Oracle Critical Patch Update Advisory - October 2020

Pony Mail!

Red Hat Customer Portal

Pony Mail!

[cassandra-commits] 20210927 [jira] [Updated] (CASSANDRA-15416) CVE-2017-7525 (jackson-databind is vulnerable to Remote Code Exec

[SECURITY] [DLA 2342-1] libjackson-json-java security update

Pony Mail!

Red Hat Customer Portal

Pony Mail!

CVE-2017-7525 Jackson JSON Library Vulnerability in NetApp Products | NetApp Product Security

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

Oracle Critical Patch Update - January 2019

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Oracle Critical Patch Update - July 2019

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

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

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

CPU Oct 2018

Red Hat Customer Portal

Apache Struts Jackson Databind Deserialization Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker

[cassandra-commits] 20210927 [jira] [Commented] (CASSANDRA-15416) CVE-2017-7525 (jackson-databind is vulnerable to Remote Code E

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

Debian -- Security Information -- DSA-4004-1 jackson-databind

Red Hat Enterprise Virtualization Multiple Flaws Let Remote Users Execute Arbitrary Code and Local Users Determine Passwords and Gain E

Red Hat Customer Portal

Pony Mail!

FasterXML Jackson-databind CVE-2017-7525 Deserialization Remote Code Execution Vulnerability

Pony Mail!

Pony Mail!

Bug 1462702 – CVE-2017-7525 jackson-databind: Deserialization vulnerability via readValue method of ObjectMapper

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - April 2019

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[980649](#) Java (maven) Security Update for com.fasterxml.jackson.core:jackson-databind (GHSA-qxxx-2pp7-5hmx)

© [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](#)