



CVE-2020-25649

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

Summary

CVE	CVE-2020-25649
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-03 17:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	lotdb	All	All	All	All
Application	Fasterxml	Jackson-databind	All	All	All	All
Application	Fasterxml	Jackson-databind	All	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Netapp	Oncommand Api Services	-	All	All	All
Application	Netapp	Oncommand Api Services	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Service Level Manager	-	All	All	All
Application	Netapp	Service Level Manager	-	All	All	All
Application	Oracle	Agile Plm	9.3.6	All	All	All
Application	Oracle	Agile Product Lifecycle Management Integration Pack	3.6	All	All	All
Application	Oracle	Banking Apis	19.1	All	All	All
Application	Oracle	Banking Apis	19.2	All	All	All
Application	Oracle	Banking Apis	20.1	All	All	All
Application	Oracle	Banking Apis	21.1	All	All	All

Application	Oracle	Banking Apis	All	All	All	All
Application	Oracle	Banking Platform	2.10.0	All	All	All
Application	Oracle	Banking Platform	2.6.2	All	All	All
Application	Oracle	Banking Platform	2.7.0	All	All	All
Application	Oracle	Banking Platform	2.7.1	All	All	All
Application	Oracle	Banking Platform	2.8.0	All	All	All
Application	Oracle	Banking Platform	2.9.0	All	All	All
Application	Oracle	Banking Treasury Management	4.4	All	All	All
Application	Oracle	Blockchain Platform	All	All	All	All
Application	Oracle	Coherence	12.2.1.4.0	All	All	All
Application	Oracle	Coherence	14.1.1.0.0	All	All	All
Application	Oracle	Commerce Platform	11.2.0	All	All	All
Application	Oracle	Commerce Platform	All	All	All	All
Application	Oracle	Communications Billing And Revenue Management	12.0.0.3.0	All	All	All
Application	Oracle	Communications Billing And Revenue Management	7.5.0.23.0	All	All	All
Application	Oracle	Communications Cloud Native Core Unified Data Repository	1.4.0	All	All	All
Application	Oracle	Communications Convergent Charging Controller	12.0.4.0.0	All	All	All
Application	Oracle	Communications Evolved Communications Application Server	7.1	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1.5.0	All	All	All
Application	Oracle	Communications Interactive Session Recorder	6.3	All	All	All
Application	Oracle	Communications Interactive Session Recorder	6.4	All	All	All
Operating System	Oracle	Communications Messaging Server	8.0.2	All	All	All
Operating System	Oracle	Communications Messaging Server	8.1	All	All	All
Application	Oracle	Communications Network Charging And Control	12.0.4.0.0	All	All	All
Application	Oracle	Communications Offline Mediation Controller	12.0.0.3	All	All	All
Application	Oracle	Communications Pricing Design Center	12.0.0.4.0	All	All	All
Application	Oracle	Communications Services Gatekeeper	7.0	All	All	All
Application	Oracle	Communications Unified Inventory Management	7.4.1	All	All	All
Application	Oracle	Goldengate Application Adapters	19.1.0.0.0	All	All	All
Application	Oracle	Health Sciences Empirica Signal	9.0	All	All	All
Application	Oracle	Health Sciences Empirica Signal	9.1	All	All	All
Application	Oracle	Insurance Policy Administration	11.0.2	All	All	All
Application	Oracle	Insurance Policy Administration	All	All	All	All
Application	Oracle	Insurance Rules Palette	11.0.2	All	All	All
Application	Oracle	Insurance Rules Palette	All	All	All	All

Application	Oracle	Jd Edwards Enterpriseone Orchestrator	All	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	All	All	All	All
Application	Oracle	Primavera Gateway	18.8	All	All	All
Application	Oracle	Primavera Gateway	19.12	All	All	All
Application	Oracle	Primavera Gateway	20.12	All	All	All
Application	Oracle	Primavera Gateway	20.12.0	All	All	All
Application	Oracle	Primavera Gateway	All	All	All	All
Application	Oracle	Primavera Gateway	All	All	All	All
Application	Oracle	Primavera Gateway	All	All	All	All
Application	Oracle	Primavera Gateway	All	All	All	All
Application	Oracle	Retail Service Backbone	14.1.3.2	All	All	All
Application	Oracle	Retail Service Backbone	15.0.3.1	All	All	All
Application	Oracle	Retail Service Backbone	16.0.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	16.0.6	All	All	All
Application	Oracle	Retail Xstore Point Of Service	17.0.4	All	All	All
Application	Oracle	Retail Xstore Point Of Service	18.0.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	19.0.2	All	All	All
Application	Oracle	Retail Xstore Point Of Service	20.0.1	All	All	All
Application	Oracle	Sd-wan Edge	9.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.5.0	All	All	All
Application	Oracle	Utilities Framework	4.3.0.6.0	All	All	All
Application	Oracle	Utilities Framework	4.4.0.0.0	All	All	All
Application	Oracle	Utilities Framework	4.4.0.2.0	All	All	All
Application	Oracle	Utilities Framework	4.4.0.3.0	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.3.0	All	All	All
Application	Oracle	Webcenter Portal	12.2.1.4.0	All	All	All
Application	Quarkus	Quarkus	All	All	All	All

References

Reference

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[kafka-dev] 20210901 Re: [EXTERNAL] Re: Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[kafka-users] 20210901 Re: [EXTERNAL] Re: Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - April 2022

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

CVE-2020-25649 FasterXML Jackson Databind Vulnerability in NetApp Products | NetApp Product Security

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - July 2021

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - October 2021

[SECURITY] Fedora 32 Update: jackson-databind-2.10.5.1-1.fc32 - package-announce - Fedora Mailing-Lists

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - January 2022

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - July 2022

Oracle Critical Patch Update Advisory - April 2021

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[kafka-dev] 20210831 Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178642](#) Debian Security Update for jackson-databind (DLA 2638-1)

[375337](#) IBM Spectrum Control Multiple Vulnerability(6415993)

[375483](#) Oracle Coherence April 2021 Critical Patch Update

[730206](#) McAfee Web Gateway Multiple Vulnerabilities (WP-3792, WP-4003, WP-4021, WP-4058, WP-4067)

[752129](#) SUSE Enterprise Linux Security Update for jackson-databind, jackson-dataformats-binary, jackson-annotations, jackson-bom, jackson-core (SUSE-SU-2022:1678-1)

[980328](#) Java (maven) Security Update for com.fasterxml.jackson.core:jackson-databind (GHSA-288c-cq4h-88gq)

© [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](#)