



# CVE-2019-12399

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

## Summary

<b>CVE</b>	CVE-2019-12399
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-14 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:03:00 UTC
<b>Description</b>	When Connect workers in Apache Kafka 2.0.0, 2.0.1, 2.1.0, 2.1.1, 2.2.0, 2.2.1, or 2.3.0 are configured with one or more cor

## Risk And Classification

**Problem Types:** CWE-319

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.0.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.0.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.1.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.2.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.2.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.3.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.0.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.0.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.1.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.1.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.2.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.2.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Kafka</a>	2.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Corporate Lending Process Management</a>	14.1.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Corporate Lending Process Management</a>	14.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Banking Corporate Lending Process Management</a>	14.4.0	All	All	All

Application	Oracle	Banking Credit Facilities Process Management	14.1.0	All	All	All
Application	Oracle	Banking Credit Facilities Process Management	14.3.0	All	All	All
Application	Oracle	Banking Credit Facilities Process Management	14.4.0	All	All	All
Application	Oracle	Banking Liquidity Management	All	All	All	All
Application	Oracle	Banking Payments	14.4.0	All	All	All
Application	Oracle	Banking Platform	2.7.0	All	All	All
Application	Oracle	Banking Supply Chain Finance	All	All	All	All
Application	Oracle	Banking Trade Finance Process Management	14.1.0	All	All	All
Application	Oracle	Banking Trade Finance Process Management	14.3.0	All	All	All
Application	Oracle	Banking Trade Finance Process Management	14.4.0	All	All	All
Application	Oracle	Banking Virtual Account Management	14.1.0	All	All	All
Application	Oracle	Banking Virtual Account Management	14.3.0	All	All	All
Application	Oracle	Banking Virtual Account Management	14.4.0	All	All	All
Application	Oracle	Blockchain Platform	All	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.9.0	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	All	All	All	All
Application	Oracle	Flexcube Universal Banking	14.4.0	All	All	All

References			
Reference	Source	Link	
Pony Mail!		<a href="#">lists.apache</a>	
Pony Mail!	MLIST	<a href="#">lists.apache</a>	
oss-security - CVE-2019-12399: Apache Kafka Connect REST API may expose plaintext secrets in tasks endpoint	MLIST	<a href="#">www.openv</a>	
Pony Mail!		<a href="#">lists.apache</a>	
Pony Mail!	MLIST	<a href="#">lists.apache</a>	
Oracle Critical Patch Update Advisory - April 2022	MISC	<a href="#">www.oracle</a>	
Pony Mail!		<a href="#">lists.apache</a>	
Pony Mail!		<a href="#">lists.apache</a>	
Pony Mail!	MLIST	<a href="#">lists.apache</a>	
Pony Mail!	MLIST	<a href="#">lists.apache</a>	
Pony Mail!		<a href="#">lists.apache</a>	
Pony Mail!	MLIST	<a href="#">lists.apache</a>	
Pony Mail!	MLIST	<a href="#">lists.apache</a>	
Pony Mail!	MLIST	<a href="#">lists.apache</a>	
Pony Mail!	MLIST	<a href="#">lists.apache</a>	

Oracle Critical Patch Update Advisory - July 2021	N/A	<a href="http://www.oracle.com">www.oracle.com</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
[kafka-commits] 20210921 [kafka-site] branch asf-site updated: Add CVE-2021-38153 (#375)		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Oracle Critical Patch Update Advisory - April 2021	MISC	<a href="http://www.oracle.com">www.oracle.com</a>
Oracle Critical Patch Update Advisory - January 2021	MISC	<a href="http://www.oracle.com">www.oracle.com</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
Pony Mail!		<a href="mailto:lists.apache@apache.org">lists.apache@apache.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

983755 Java (maven) Security Update for org.apache.kafka:kafka (GHS-6jmf-mxwf-r3jc)

© [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](#)**