



# CVE-2021-38153

Published on: 09/22/2021 12:00:00 AM UTC

Last Modified on: 10/05/2022 06:23:00 PM UTC

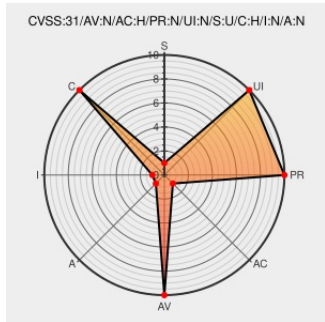
## CVE-2021-38153

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Kafka](#) from [Apache](#) contain the following vulnerability:

Some components in Apache Kafka use `Arrays.equals` to validate a password or key, which is vulnerable to timing attacks that make brute force attacks for such credentials more likely to be successful. Users should upgrade to 2.8.1 or higher, or 3.0.0 or higher where this vulnerability has been fixed. The affected versions include Apache

Kafka 2.0.0, 2.0.1, 2.1.0, 2.1.1, 2.2.0, 2.2.1, 2.2.2, 2.3.0, 2.3.1, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, and 2.8.0.

CVE-2021-38153 has been assigned by security@apache.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>HIGH</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>NONE</b>	<b>NONE</b>

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>NONE</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Deny Mail		MITST (kafka-issues) 2021-10-12 [NOTE] 2.7.3 DO...

Pony Mail!	<a href="https://lists.apache.org">lists.apache.org</a> text/html	MLIST [kafka-users] 20211012 [VOTE] 2.7.2 RC0
Pony Mail!	<a href="https://lists.apache.org">lists.apache.org</a> text/html	MLIST [kafka-dev] 20211007 Re: CVE Back Port?
Pony Mail!	<a href="https://lists.apache.org">lists.apache.org</a> text/html	MLIST [kafka-users] 20211012 [VOTE] 2.6.3 RC0
Oracle Critical Patch Update Advisory - April 2022	<a href="https://www.oracle.com">www.oracle.com</a> text/html	MISC <a href="https://www.oracle.com/security-alerts/cpuapr2022.html">www.oracle.com/security-alerts/cpuapr2022.html</a>
Pony Mail!	<a href="https://lists.apache.org">lists.apache.org</a> text/html	MLIST [kafka-dev] 20211012 [VOTE] 2.6.3 RC0
Oracle Critical Patch Update Advisory - January 2022	<a href="https://www.oracle.com">www.oracle.com</a> text/html	MISC <a href="https://www.oracle.com/security-alerts/cpujan2022.html">www.oracle.com/security-alerts/cpujan2022.html</a>
Pony Mail!	<a href="https://lists.apache.org">lists.apache.org</a> text/html	MLIST [kafka-dev] 20211026 Re: [kafka-clients] [VOTE] 2.7.2 RC0
Apache Kafka	<a href="https://kafka.apache.org">kafka.apache.org</a> text/html	MISC <a href="https://kafka.apache.org/cve-list">kafka.apache.org/cve-list</a>
Pony Mail!	<a href="https://lists.apache.org">lists.apache.org</a> text/html	MLIST [kafka-dev] 20211012 [VOTE] 2.7.2 RC0
Pony Mail!	<a href="https://lists.apache.org">lists.apache.org</a> text/html	MLIST [kafka-users] 20211026 Re: [kafka-clients] [VOTE] 2.7.2 RC0
Oracle Critical Patch Update Advisory - July 2022	<a href="https://www.oracle.com">www.oracle.com</a> text/html	MISC <a href="https://www.oracle.com/security-alerts/cpujul2022.html">www.oracle.com/security-alerts/cpujul2022.html</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

## Related QID Numbers

[375930](#) Apache Kafka Timing Attack Vulnerability

[983504](#) Java (maven) Security Update for org.apache.kafka:kafka (GHSA-3j6g-hxx5-3q26)

## Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Kafka	All	All	All	All
Application	Apache	Kafka	2.8.0	-	All	All
Application	Oracle	Communications Brm - Elastic Charging Engine	All	All	All	All
Application	Oracle	Communications Brm - Elastic Charging Engine	12.0.0.5.0	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.15.0	All	All	All



Application	Oracle	Financial Services Analytical Applications Infrastructure	All	All	All	All
Application	Oracle	Financial Services Analytical Applications Infrastructure	All	All	All	All
Application	Oracle	Financial Services Behavior Detection Platform	8.1.1.0	All	All	All
Application	Oracle	Financial Services Behavior Detection Platform	8.1.1.1	All	All	All
Application	Oracle	Financial Services Behavior Detection Platform	8.1.2.0	All	All	All
Application	Oracle	Financial Services Behavior Detection Platform	All	All	All	All
Application	Oracle	Financial Services Enterprise Case Management	8.0.7.1	All	All	All
Application	Oracle	Financial Services Enterprise Case Management	8.0.7.2	All	All	All
Application	Oracle	Financial Services Enterprise Case Management	8.0.8.0	All	All	All
Application	Oracle	Financial Services Enterprise Case Management	8.0.8.1	All	All	All
Application	Oracle	Financial Services Enterprise Case Management	8.1.1.0	All	All	All
Application	Oracle	Financial Services Enterprise Case Management	8.1.1.1	All	All	All
Application	Oracle	Primavera Unifier	18.8	All	All	All
Application	Oracle	Primavera Unifier	19.12	All	All	All
Application	Oracle	Primavera Unifier	20.12	All	All	All
Application	Oracle	Primavera Unifier	21.12	All	All	All
Application	Quarkus	Quarkus	All	All	All	All
cpe:2.3:a:apache:kafka:****:*:*:						
cpe:2.3:a:apache:kafka:2.8.0:-:*:*:*:*:						
cpe:2.3:a:oracle:communications_brm_-_elastic_charging_engine:****:*:*:						
cpe:2.3:a:oracle:communications_brm_-_elastic_charging_engine:12.0.0.5.0:*:*:*:*:*:						
cpe:2.3:a:oracle:communications_cloud_native_core_policy:1.15.0:****:*:*:						
cpe:2.3:a:oracle:financial_services_analytical_applications_infrastructure:****:*:*:						
cpe:2.3:a:oracle:financial_services_analytical_applications_infrastructure:****:*:*:						
cpe:2.3:a:oracle:financial_services_behavior_detection_platform:8.1.1.0:****:*:*:						
cpe:2.3:a:oracle:financial_services_behavior_detection_platform:8.1.1.1:*:*:*:*:*:						
cpe:2.3:a:oracle:financial_services_behavior_detection_platform:8.1.2.0:****:*:*:						
cpe:2.3:a:oracle:financial_services_behavior_detection_platform:*:*:*:*:*:						
cpe:2.3:a:oracle:financial_services_enterprise_case_management:8.0.7.1:****:*:*:						
cpe:2.3:a:oracle:financial_services_enterprise_case_management:8.0.7.2:****:*:*:						
cpe:2.3:a:oracle:financial_services_enterprise_case_management:8.0.8.0:****:*:*:						
cpe:2.3:a:oracle:financial_services_enterprise_case_management:8.0.8.1:****:*:*:						

cpe:2.3:a:oracle:financial_services_enterprise_case_management:8.1.1.0:****:*:*:
cpe:2.3:a:oracle:financial_services_enterprise_case_management:8.1.1.1:****:*:*:
cpe:2.3:a:oracle:primavera_unifier:18.8:****:*:*:
cpe:2.3:a:oracle:primavera_unifier:19.12:****:*:*:
cpe:2.3:a:oracle:primavera_unifier:20.12:****:*:*:
cpe:2.3:a:oracle:primavera_unifier:21.12:****:*:*:
cpe:2.3:a:quarkus:quarkus:****:*:*:

Discovery Credit

Apache Kafka would like to thank J. Santilli for reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
 @oss_security	CVE-2021-38153: Timing Attack Vulnerability for Apache Kafka Connect and Clients: Posted by Randall Hauch on Sep 21... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-09-21 18:40:32
 @CVereport	CVE-2021-38153 : Some components in #Apache Kafka use `Arrays.equals` to validate a password or key, which is vulne... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-09-22 09:09:59
 @threatmeter	CVE-2021-38153 Some components in Apache Kafka use `Arrays.equals` to validate a password or key, which is vulnerab... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-09-23 07:09:50

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](https://status.cve.report)**