



CVE-2021-28168

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

Summary

CVE	CVE-2021-28168
State	PUBLIC
Assigner	security@eclipse.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-22 18:15:00 UTC
Updated	2023-11-07 03:32:00 UTC
Description	Eclipse Jersey 2.28 to 2.33 and Eclipse Jersey 3.0.0 to 3.0.1 contains a local information disclosure vulnerability. This is du

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eclipse	Jersey	All	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.15.0	All	All	All
Application	Oracle	Communications Cloud Native Core Unified Data Repository	1.15.0	All	All	All

References

Reference
Pony Mail!
[kafka-jira] 20210507 [GitHub] [kafka] dongjinleekr commented on pull request #10641: KAFKA-12752: CVE-2021-28168 upgrade jersey to 2.34
Pony Mail!
[kafka-jira] 20210505 [GitHub] [kafka] shayelkin opened a new pull request #10636: MINOR: Bump Jersey deps to 2.34 due to CVE-2021-28168
[kafka-jira] 20210506 [jira] [Commented] (KAFKA-12752) CVE-2021-28168 upgrade jersey to 2.34 or 3.02
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Oracle Critical Patch Update Advisory - April 2022
Pony Mail!

Pony Mail!

[kafka-commits] 20210506 [kafka] branch 2.7 updated: KAFKA-12752: Bump Jersey deps to 2.34 due to CVE-2021-28168 (#10636)

Pony Mail!

Pony Mail!

[kafka-jira] 20210507 [GitHub] [kafka] dongjinleekr closed pull request #10641: KAFKA-12752: CVE-2021-28168 upgrade jersey to 2.34 or 3.0

[kafka-jira] 20210506 [jira] [Resolved] (KAFKA-12752) CVE-2021-28168 upgrade jersey to 2.34 or 3.02

[kafka-dev] 20210506 [jira] [Resolved] (KAFKA-12752) CVE-2021-28168 upgrade jersey to 2.34 or 3.02

[kafka-jira] 20210506 [jira] [Assigned] (KAFKA-12752) CVE-2021-28168 upgrade jersey to 2.34 or 3.02

Pony Mail!

Pony Mail!

Pony Mail!

[kafka-dev] 20210505 [jira] [Created] (KAFKA-12752) CVE-2021-28168 upgrade jersey to 2.34 or 3.02

[kafka-jira] 20210506 [GitHub] [kafka] omkreddy commented on pull request #10641: KAFKA-12752: CVE-2021-28168 upgrade jersey to 2.34

[kafka-jira] 20210506 [GitHub] [kafka] omkreddy merged pull request #10636: MINOR: Bump Jersey deps to 2.34 due to CVE-2021-28168

switching to NIO tmp file creation approach by senivam · Pull Request #4712 · eclipse-ee4j/jersey · GitHub

Pony Mail!

Pony Mail!

[kafka-jira] 20210506 [GitHub] [kafka] dongjinleekr opened a new pull request #10641: KAFKA-12752: CVE-2021-28168 upgrade jersey to 2.3

Local information disclosure via system temporary directory · Advisory · eclipse-ee4j/jersey · GitHub

[kafka-users] 20210617 vulnerabilities

Pony Mail!

[kafka-jira] 20210505 [jira] [Created] (KAFKA-12752) CVE-2021-28168 upgrade jersey to 2.34 or 3.02

[kafka-commits] 20210506 [kafka] branch 2.8 updated: KAFKA-12752: Bump Jersey deps to 2.34 due to CVE-2021-28168 (#10636)

[kafka-jira] 20210429 [GitHub] [kafka] xjin-Confluent opened a new pull request #10614: MINOR: Upgrade jersey to 2.34

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[150696](#) Oracle WebLogic Server Multiple Vulnerabilities (CPUJUL2023)

[87546](#) Oracle WebLogic Server Multiple Vulnerabilities (CPUJUL2023)

[982091](#) Java (maven) Security Update for org.glassfish.jersey.core:jersey-common (GHSA-c43q-5hpj-4crv)

© [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](#)