# CVE-2019-17571

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2019-17571 |
| **State** | PUBLIC |
| **Assigner** | security@apache.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2019-12-20 17:15:00 UTC |
| **Updated** | 2023-11-07 03:06:00 UTC |
| **Description** | Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited t |

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Apache | Bookkeeper | All | All | All | All |
| Application | Apache | Log4j | All | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | 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 | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Netapp | Oncommand System Manager | All | All | All | All |
| Application | Netapp | Oncommand Workflow Automation | - | All | All | All |
| Application | Netapp | Oncommand Workflow Automation | - | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Application | Oracle | Application Testing Suite | 13.3.0.1 | All | All | All |
| Application | Oracle | Application Testing Suite | 13.3.0.1 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Oracle | Communications Network Integrity | All | All | All | All |
| Application | Oracle | Endeca Information Discovery Studio | 3.2.0 | All | All | All |
| Application | Oracle | Endeca Information Discovery Studio | 3.2.0 | All | All | All |
| Application | Oracle | Financial Services Lending And Leasing | 12.5.0 | All | All | All |
| Application | Oracle | Financial Services Lending And Leasing | 12.5.0 | All | All | All |
| Application | Oracle | Financial Services Lending And Leasing | All | All | All | All |
| Application | Oracle | Mysql Enterprise Monitor | All | All | All | All |
| Application | Oracle | Primavera Gateway | All | All | All | All |
| Application | Oracle | Primavera Gateway | All | All | All | All |
| Application | Oracle | Rapid Planning | 12.1 | All | All | All |
| Application | Oracle | Rapid Planning | 12.2 | All | All | All |
| Application | Oracle | Rapid Planning | 12.1 | All | All | All |
| Application | Oracle | Rapid Planning | 12.2 | All | All | All |
| Application | Oracle | Retail Extract Transform And Load | 19.0 | All | All | All |
| Application | Oracle | Retail Extract Transform And Load | 19.0 | All | All | All |
| Application | Oracle | Retail Service Backbone | 14.1 | All | All | All |
| Application | Oracle | Retail Service Backbone | 15.0 | All | All | All |
| Application | Oracle | Retail Service Backbone | 16.0 | All | All | All |
| Application | Oracle | Retail Service Backbone | 14.1 | All | All | All |
| Application | Oracle | Retail Service Backbone | 15.0 | All | All | All |
| Application | Oracle | Retail Service Backbone | 16.0 | All | All | All |
| Application | Oracle | Weblogic Server | 10.3.6.0.0 | All | All | All |
| Application | Oracle | Weblogic Server | 12.1.3.0.0 | All | All | All |
| Application | Oracle | Weblogic Server | 12.2.1.3.0 | All | All | All |
| Application | Oracle | Weblogic Server | 12.2.1.4.0 | All | All | All |
| Application | Oracle | Weblogic Server | 14.1.1.0.0 | All | All | All |
| Application | Oracle | Weblogic Server | 10.3.6.0.0 | All | All | All |
| Application | Oracle | Weblogic Server | 12.1.3.0.0 | All | All | All |
| Application | Oracle | Weblogic Server | 12.2.1.3.0 | All | All | All |
| Application | Oracle | Weblogic Server | 12.2.1.4.0 | All | All | All |
| Application | Oracle | Weblogic Server | 14.1.1.0.0 | All | All | All |

## References

| Reference |
|---|
| Pony Mail! |

Pony Mail!

Pony Mail!

Pony Mail!

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!

[bookkeeper-issues] 20211007 [GitHub] [bookkeeper] RaulGracia commented on a change in pull request #2816: Issue 2815: Upgrade to log4

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!

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 - July 2020

Pony Mail!

Pony Mail!

Oracle Critical Patch Update Advisory - April 2022

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[hadoop-common-issues] 20211006 [jira] [Commented] (HADOOP-17221) update log4j-1.2.17 to atlassian version( To Address: CVE-2019-17

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[security-announce] openSUSE-SU-2020:0051-1: important: Security update

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[bookkeeper-issues] 20211016 [GitHub] [bookkeeper] pkumar-singh commented on a change in pull request #2816: Issue 2815: Upgrade to lo

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[bookkeeper-issues] 20211006 [GitHub] [bookkeeper] RaulGracia opened a new issue #2815: Upgrade to log4j2 to get rid of CVE-2019-17571

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!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[bookkeeper-issues] 20211017 [GitHub] [bookkeeper] eolivelli commented on a change in pull request #2816: Issue 2815: Upgrade to log4j2 t

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Debian -- Security Information -- DSA-4686-1 apache-log4j1.2

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!

Pony Mail!

Pony Mail!

[bookkeeper-issues] 20211006 [GitHub] [bookkeeper] eolivelli commented on a change in pull request #2816: Issue 2815: Upgrade to log4j2 t

Pony Mail!

[bookkeeper-issues] 20211013 [GitHub] [bookkeeper] eolivelli commented on pull request #2816: Issue 2815: Upgrade to log4j2 to get rid of C

[bookkeeper-issues] 20211018 [GitHub] [bookkeeper] RaulGracia commented on pull request #2816: Issue 2815: Upgrade to log4j2 to get rid

USN-4495-1: Apache Log4j vulnerability | Ubuntu security notices | Ubuntu

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[SECURITY] [DLA 2065-1] apache-log4j1.2 security update

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!

[activemq-users] 20210427 Release date for ActiveMQ v5.16.2 to fix CVEs

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[kafka-users] 20210831 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!

[kafka-users] 20210617 vulnerabilities

Pony Mail!

Pony Mail!

[bookkeeper-issues] 20211017 [GitHub] [bookkeeper] zymap commented on pull request #2816: Issue 2815: Upgrade to log4j2 to get rid of C

Pony Mail!

Pony Mail!

Pony Mail!

[bookkeeper-issues] 20211007 [GitHub] [bookkeeper] eolivelli commented on a change in pull request #2816: Issue 2815: Upgrade to log4j2 t

[bookkeeper-issues] 20211006 [GitHub] [bookkeeper] RaulGracia opened a new pull request #2816: Issue 2815: Upgrade to log4j2 to get rid o

Pony Mail!

Oracle Critical Patch Update Advisory - April 2020

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-2019-17571 Apache Log4j Vulnerability in NetApp Products | NetApp Product Security

Pony Mail!

Pony Mail!

Pony Mail!

[mina-dev] 20210225 [jira] [Created] (FTPSERVER-500) Security vulnerability in common/lib/log4j-1.2.17.jar

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!

[bookkeeper-commits] 20211014 [bookkeeper] branch master updated: Issue 2815: Upgrade to log4j2 to get rid of CVE-2019-17571 (#2816)

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

[bookkeeper-issues] 20211007 [GitHub] [bookkeeper] RaulGracia commented on pull request #2816: Issue 2815: Upgrade to log4j2 to get rid

Pony Mail!

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

Pony Mail!

Pony Mail!

Pony Mail!

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

199275 Ubuntu Security Notification for Apache Log4j Vulnerabilities (USN-5998-1)

353112 Amazon Linux Security Advisory for log4j : ALAS-2022-1562

372577 IBM Spectrum Control (Tivoli Storage Productivity Center) Apache Log4j vulnerability (1488939)

980407 Java (maven) Security Update for log4j:log4j (GHSA-2qrg-x229-3v8q)

© 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 registred 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.

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status status.cve.report**