



CVE-2020-14798

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-14798
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-21 15:15:00 UTC
Updated	2022-05-13 14:57:00 UTC
Description	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions the

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	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	9.0	All	All	All
Application	Netapp	7-mode Transition Tool	-	All	All	All
Application	Netapp	7-mode Transition Tool	-	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	E-series Santricity Os Controller	All	All	All	All
Application	Netapp	E-series Santricity Storage Manager	-	All	All	All
Application	Netapp	E-series Santricity Storage Manager	-	All	All	All
Application	Netapp	E-series Santricity Web Services Proxy	-	All	All	All
Application	Netapp	E-series Santricity Web Services Proxy	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All

Hardware	Netapp	Hci Storage Node	-	All	All	All
Hardware	Netapp	Hci Storage Node	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Santricity Cloud Connector	-	All	All	All
Application	Netapp	Santricity Cloud Connector	-	All	All	All
Application	Netapp	Santricity Unified Manager	-	All	All	All
Application	Netapp	Santricity Unified Manager	-	All	All	All
Application	Netapp	Snapmanager	-	-	All	All
Application	Netapp	Snapmanager	-	-	All	All
Application	Netapp	Snapmanager	-	-	All	All
Application	Netapp	Snapmanager	-	-	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Oracle	Jdk	1.7.0	update271	All	All
Application	Oracle	Jdk	1.8.0	update261	All	All
Application	Oracle	Jdk	11.0.8	All	All	All
Application	Oracle	Jdk	15	All	All	All
Application	Oracle	Jdk	1.7.0	update271	All	All
Application	Oracle	Jdk	1.8.0	update261	All	All
Application	Oracle	Jdk	11.0.8	All	All	All
Application	Oracle	Jdk	15	All	All	All
Application	Oracle	Jre	1.8.0	update261	All	All
Application	Oracle	Jre	1.8.0	update_261	All	All
Application	Oracle	Jre	1.8.0	update_261	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-4779-1 openjdk-11	DEBIAN	www.debian.org
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com
[SECURITY] [DLA 2412-1] openjdk-8 security update	MLIST	lists.debian.org

OpenJDK: Multiple vulnerabilities (GLSA 202101-19) — Gentoo security	GENIOO	security.gentoo.org
[security-announce] openSUSE-SU-2020:1893-1: important: Security update	SUSE	lists.opensuse.org
October 2020 Java Platform Standard Edition Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [330080](#) IBM AIX Java Multiple Vulnerabilities (java_mar2021_advisory)
- [375285](#) EulerOS Security Update for java-1.8.0-openjdk (EulerOS-SA-2021-1310)
- [375466](#) IBM CICS Transaction Gateway Multiple Vulnerabilities
- [375815](#) Azul Java Multiple Vulnerabilities Security Update October2020
- [375983](#) Amazon Corretto Critical Patch Update (OCT2020)
- [501104](#) Alpine Linux Security Update for openjdk8
- [501206](#) Alpine Linux Security Update for openjdk11
- [501214](#) Alpine Linux Security Update for openjdk7
- [501650](#) Alpine Linux Security Update for openjdk7
- [670417](#) EulerOS Security Update for java-1.8.0-openjdk (EulerOS-SA-2021-1982)
- [670462](#) EulerOS Security Update for java-1.8.0-openjdk (EulerOS-SA-2021-2220)
- [670859](#) EulerOS Security Update for java-1.8.0-openjdk (EulerOS-SA-2021-1982)
- [750542](#) OpenSUSE Security Update for java-1_8_0-openjdk (openSUSE-SU-2020:2083-1)
- [750556](#) OpenSUSE Security Update for java-1_8_0-openjdk (openSUSE-SU-2020:2048-1)
- [750579](#) OpenSUSE Security Update for java-11-openjdk (openSUSE-SU-2020:1994-1)
- [750585](#) OpenSUSE Security Update for java-11-openjdk (openSUSE-SU-2020:1984-1)

© [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](#)