

Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Oncommand Workflow Automation	All	All	All	All
Application	Netapp	Oncommand Workflow Automation	All	All	All	All
Application	Netapp	Snapmanager	All	All	All	All
Application	Netapp	Snapmanager	All	All	All	All
Application	Netapp	Snapmanager	All	All	All	All
Application	Netapp	Snapmanager	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Application	Oracle	Jdk	1.7.0	update201	All	All
Application	Oracle	Jdk	1.8.0	update192	All	All
Application	Oracle	Jdk	11.0.1	All	All	All
Application	Oracle	Jdk	1.7.0	update201	All	All
Application	Oracle	Jdk	1.8.0	update192	All	All
Application	Oracle	Jdk	11.0.1	All	All	All
Application	Oracle	Jre	8.0	update_191	All	All
Application	Oracle	Jre	8.0	update_191	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Satellite	5.8	All	All	All
Application	Redhat	Satellite	5.8	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	access.redhat.com
SECURITY DATA CENTER: HOW TO PROTECT YOUR DATA	MICROSOFT	https://www.microsoft.com/en-us/security/default

[SECURITY] [DLA 1638-1] libjpeg-turbo security update	MLISI	lists.debian.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com
Red Hat Customer Portal	REDHAT	access.redhat.com
[security-announce] openSUSE-SU-2019:0346-1: important: Security update	SUSE	lists.opensuse.org
January 2019 Java Platform Standard Edition Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
security_advisories/libjpeg-v9a at master · ChijinZ/security_advisories · GitHub	MISC	github.com
GitHub - zzyyrr/divide-by-zero-in-libjpeg-9d: Divide-by-zero in libjpeg-9d	MISC	github.com
USN-3706-2: libjpeg-turbo vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Oracle Critical Patch Update - January 2019	CONFIRM	www.oracle.com
USN-3706-1: libjpeg-turbo vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
Oracle Java SE CVE-2018-11212 Remote Security Vulnerability	BID	www.securityfocus.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Document Display HPE Support Center	CONFIRM	support.hpe.com
[security-announce] openSUSE-SU-2019:1439-1: important: Security update	SUSE	lists.opensuse.org
[security-announce] openSUSE-SU-2019:1500-1: moderate: Security update f	SUSE	lists.opensuse.org
Independent JPEG Group	MISC	www.ijg.org
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

[377472](#) Alibaba Cloud Linux Security Update for libjpeg-turbo (ALINUX2-SA-2019:0070)

[501208](#) Alpine Linux Security Update for openjdk7

[501217](#) Alpine Linux Security Update for openjdk8

© 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](#).

