



CVE-2021-4213

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

Summary

CVE	CVE-2021-4213
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-24 16:15:00 UTC
Updated	2022-08-29 13:19:00 UTC
Description	A flaw was found in JSS, where it did not properly free up all memory. Over time, the wasted memory builds up in the serve

Risk And Classification

Problem Types: CWE-401

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	11.0	All	All	All
Application	Dogtagpki	Network Security Services For Java	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
Fix memory leak on each TLS connection · dogtagpki/jss@5922560 · GitHub	MISC	github.com
CVE-2021-4213	MISC	security-tracker.debian.org
2042900 – (CVE-2021-4213) CVE-2021-4213 JSS: memory leak in TLS connection leads to OOM	MISC	bugzilla.redhat.com
Additional fix for TLS connection I missed from original patch · dogtagpki/jss@3aabe0e · GitHub	MISC	github.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.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

159837 Oracle Enterprise Linux Security Update for pki-core:10.6 (ELSA-2022-1851)

182303 Debian Security Update for jss (CVE-2021-4213)

240289 Red Hat Update for pki-core:10.6 (RHSA-2022:1851)

940497 AlmaLinux Security Update for pki-core:10.6 (ALSA-2022:1851)

960436 Rocky Linux Security Update for pki-core:10.6 (RLSA-2022:1851)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)