



CVE-2022-2414

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

Summary

CVE	CVE-2022-2414
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-29 19:15:00 UTC
Updated	2022-08-04 20:25:00 UTC
Description	Access to external entities when parsing XML documents can lead to XML external entity (XXE) attacks. This flaw allows a

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dogtagpki	Dogtagpki	10.11.2	All	All	All
Application	Dogtagpki	Dogtagpki	10.12.4	All	All	All
Application	Dogtagpki	Dogtagpki	10.5.18	All	All	All
Application	Dogtagpki	Dogtagpki	10.7.4	All	All	All
Application	Dogtagpki	Dogtagpki	10.8.3	All	All	All
Application	Dogtagpki	Dogtagpki	11.0.5	All	All	All
Application	Dogtagpki	Dogtagpki	11.1.0	All	All	All

References

Reference	Source	Link
Disable access to external entities when parsing XML by ckelleyRH · Pull Request #4021 · dogtagpki/pki · GitHub	MISC	github.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

160198 Oracle Enterprise Linux Security Update for pki-core (ELSA-2022-7326)
160225 Oracle Enterprise Linux Security Update for pki-core:10.6 and pki-deps:10.6 (ELSA-2022-7470)
160344 Oracle Enterprise Linux Security Update for pki-core (ELSA-2022-8799)
240806 Red Hat Update for pki-core (RHSA-2022:7326)
240845 Red Hat Update for pki-core:10.6 and pki-deps:10.6 (RHSA-2022:7470)
240964 Red Hat Update for pki-core (RHSA-2022:8799)
241378 Red Hat Update for pki-core:10.6 (RHSA-2023:1966)
241564 Red Hat Update for pki-core:10.6 (RHSA-2023:3394)
241675 Red Hat Update for pki-core:10.6 (RHSA-2023:1747)
257217 CentOS Security Update for pki-core (CESA-2022:8799)
354895 Amazon Linux Security Advisory for pki-core : ALAS2-2023-2016
377787 Alibaba Cloud Linux Security Update for pki-core:10.6 and pki-deps:10.6 (ALINUX3-SA-2022:0184)
377849 Alibaba Cloud Linux Security Update for pki-core (ALINUX2-SA-2022:0057)
673071 EulerOS Security Update for pki-core (EulerOS-SA-2023-2164)
673078 EulerOS Security Update for pki-core (EulerOS-SA-2023-2197)
940725 AlmaLinux Security Update for pki-core (ALSA-2022:7326)
940764 AlmaLinux Security Update for pki-core:10.6 and pki-deps:10.6 (ALSA-2022:7470)
960545 Rocky Linux Security Update for pki-core:10.6 and pki-deps:10.6 (RLSA-2022:7470)
960564 Rocky Linux Security Update for pki-core (RLSA-2022:7326)

© [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](#)