



CVE-2021-23792

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

Summary

CVE	CVE-2021-23792
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-06 20:15:00 UTC
Updated	2022-05-17 17:20:00 UTC
Description	The package com.twelvemonkeys.imageio:imageio-metadata before 3.7.1 are vulnerable to XML External Entity (XXE) Inje

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Twelvemonkeys Project	Twelvemonkeys	All	All	All	All

References

Reference	Source	Link
XML External Entity (XXE) Injection in com.twelvemonkeys.imageio:imageio-metadata CVE-2021-23792 Snyk	CONFIRM	snyk.io
Avoid fetching external resources in XMPReader. · haraldk/TwelveMonkeys@da4efe9 · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: MOGWAI LABS GmbH

LEGACY: Timo Müller

Legacy QID Mappings

[182511](#) Debian Security Update for libtwelvemonkeys-java (CVE-2021-23792)

© [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](#)