



# CVE-2019-20421

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

## Summary

<b>CVE</b>	CVE-2019-20421
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-27 05:15:00 UTC
<b>Updated</b>	2021-09-14 12:46:00 UTC
<b>Description</b>	In Jp2Image::readMetadata() in jp2image.cpp in Exiv2 0.27.2, an input file can result in an infinite loop and hang, with high

## Risk And Classification

**Problem Types:** CWE-835

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Exiv2</a>	<a href="#">Exiv2</a>	0.27.2	All	All	All
Application	<a href="#">Exiv2</a>	<a href="#">Exiv2</a>	0.27.2	All	All	All

## References

Reference	Source	Link	Tags
Fix #1011 fix_1011_jp2_readmetadata_loop (#1013) · Exiv2/exiv2@a82098f · GitHub	MISC	<a href="#">github.com</a>	Patch, Tr
An infinite loop and hang in Exiv2::Jp2Image::readMetadata() · Issue #1011 · Exiv2/exiv2 · GitHub	MISC	<a href="#">github.com</a>	Exploit, P
Debian -- Security Information -- DSA-4958-1 exiv2	DEBIAN	<a href="#">www.debian.org</a>	
[SECURITY] [DLA 2750-1] exiv2 security update	MLIST	<a href="#">lists.debian.org</a>	

USN-4270-1: Exiv2 vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Par
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[178761](#) Debian Security Update for exiv2 (DSA 4958-1)

[178777](#) Debian Security Update for exiv2 (DLA 2750-1)

[500895](#) Alpine Linux Security Update for exiv2

[504729](#) Alpine Linux Security Update for exiv2

[901387](#) Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7205)

[902276](#) Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7205-1)

[940399](#) AlmaLinux Security Update for exiv2 (ALSA-2020:1577)

[960313](#) Rocky Linux Security Update for exiv2 (RLSA-2020:1577)

© [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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)