



CVE-2018-10772

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-10772
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-07 02:29:00 UTC
Updated	2019-08-06 17:15:00 UTC
Description	The tEXtToDataBuf function in pngimage.cpp in Exiv2 through 0.26 allows remote attackers to cause a denial of service (ar

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exiv2	Exiv2	All	All	All	All

References

Reference	Source	Link
1566260 – There is a Segmentation fault in the software exiv2 when the function Exiv2::tEXtToDataBuf() is finished	MISC	bugzilla.re
Red Hat Customer Portal	REDHAT	access.red
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377485](#) Alibaba Cloud Linux Security Update for exiv2 (ALINUX2-SA-2019:0103)

[752681](#) SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:3598-1)

[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](#)

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