



CVE-2018-8977

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

Summary

CVE	CVE-2018-8977
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-25 03:29:00 UTC
Updated	2019-08-06 17:15:00 UTC
Description	In Exiv2 0.26, the Exiv2::Internal::printCsLensFFFF function in canonmn_int.cpp allows remote attackers to cause a denial of service (CPU consumption) via crafted XMP metadata.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exiv2	Exiv2	0.26	All	All	All
Application	Exiv2	Exiv2	0.26	All	All	All

References

Reference	Source	Link	Tags
Invalid memory access in Exiv2::Internal::printCsLensFFFF · Issue #247 · Exiv2/exiv2 · GitHub	MISC	github.com	Exploit, Issue
Exiv2: Multiple vulnerabilities (GLSA 201811-14) — Gentoo security	GENTOO	security.gentoo.org	Third Party
Red Hat Customer Portal	REDHAT	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

[710310](#) Gentoo Linux Exiv2 Multiple Vulnerabilities (GLSA 201811-14)

[750004](#) CVE-2018-8977: Exiv2 Multiple Vulnerabilities (CVE-2018-8977)

© [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](#)