



CVE-2020-18773

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

Summary

CVE	CVE-2020-18773
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-23 22:15:00 UTC
Updated	2023-12-22 10:15:00 UTC
Description	An invalid memory access in the decode function in iptc.cpp of Exiv2 0.27.99.0 allows attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exiv2	Exiv2	0.27.99.0	All	All	All

References

Reference	Source	Link	Tags
Exiv2: Multiple Vulnerabilities (GLSA 202312-06) — Gentoo security		security.gentoo.org	
one invalid memory access in decode function in iptc.cpp · Issue #760 · Exiv2/exiv2 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710810 Gentoo Linux Exiv2 Multiple Vulnerabilities (GLSA 202312-06)

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