



CVE-2018-12265

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

Summary

CVE	CVE-2018-12265
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-13 11:29:00 UTC
Updated	2019-08-06 17:15:00 UTC
Description	Exiv2 0.26 has an integer overflow in the LoaderExifJpeg class in preview.cpp, leading to an out-of-bounds read in Exiv2::M

Risk And Classification

Problem Types: CWE-125 | CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Exiv2	Exiv2	0.26	All	All	All
Application	Exiv2	Exiv2	0.26	All	All	All

References

Reference	Source	Link	Tags
-----------	--------	------	------

Debian -- Security Information -- DSA-4238-1 exiv2	DEBIAN	www.debian.org	Third Pa
pocs/1-out-of-read-Poc at master · TeamSerious/pocs · GitHub	CONFIRM	github.com	Exploit,
USN-3700-1: Exiv2 vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Pa
Exiv2: Multiple vulnerabilities (GLSA 201811-14) — Gentoo security	GENTOO	security.gentoo.org	Third Pa
[security-announce] openSUSE-SU-2020:0482-1: moderate: Security update f	SUSE	lists.opensuse.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
[SECURITY] [DLA 1402-1] exiv2 security update	MLIST	lists.debian.org	Third Pa
out of bound read when extract preview images from Poc file · Issue #365 · Exiv2/exiv2 · GitHub	CONFIRM	github.com	Exploit,
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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