



# CVE-2018-20097

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-20097
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-12 10:29:00 UTC
<b>Updated</b>	2023-11-07 02:56:00 UTC
<b>Description</b>	There is a SEGV in Exiv2::Internal::TiffParserWorker::findPrimaryGroups of tiffimage_int.cpp in Exiv2 0.27-RC3. A crafted i

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Exiv2</a>	<a href="#">Exiv2</a>	0.27	rc3	All	All
Application	<a href="#">Exiv2</a>	<a href="#">Exiv2</a>	0.27	rc3	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Dekstop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link
[SECURITY] [DLA 3265-1] exiv2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] [DLA 1691-1] exiv2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 30 Update: mingw-exiv2-0.27-3.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
pocs/exiv2/20181206 at master · TeamSeri0us/pocs · GitHub	MISC	<a href="https://github.com">github.com</a>
[SECURITY] Fedora 30 Update: mingw-exiv2-0.27-3.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>

Several bugs in exiv2 0.27-rc3 · Issue #590 · Exiv2/exiv2 · GitHub	MISC	<a href="https://github.com">github.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

- [181464](#) Debian Security Update for exiv2 (DLA 3265-1)
- [377485](#) Alibaba Cloud Linux Security Update for exiv2 (ALINUX2-SA-2019:0103)
- [752871](#) SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:4252-1)
- [752916](#) SUSE Enterprise Linux Security Update for exiv2-0\_26 (SUSE-SU-2022:4208-1)
- [752954](#) SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:4276-1)
- [940399](#) AlmaLinux Security Update for exiv2 (ALSA-2020:1577)
- [960313](#) Rocky Linux Security Update for exiv2 (RLSA-2020:1577)

© [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](https://cve.report/api)

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