



# CVE-2020-13113

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

## Summary

<b>CVE</b>	CVE-2020-13113
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-21 17:15:00 UTC
<b>Updated</b>	2022-04-26 20:50:00 UTC
<b>Description</b>	An issue was discovered in libexif before 0.6.22. Use of uninitialized memory in EXIF Makernote handling could lead to crash.

## Risk And Classification

**Problem Types:** CWE-908

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	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="#">Libexif Project</a>	<a href="#">Libexif</a>	All	All	All	All
Application	<a href="#">Libexif Project</a>	<a href="#">Libexif</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:0793-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
[SECURITY] [DLA 2222-1] libexif security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing L
USN-4396-1: libexif vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	

Ensure the MakerNote data pointers are initialized with NULL. · libexif/libexif@ec412aa · GitHub	MISC	<a href="https://github.com">github.com</a>	Patch, T
libexif: Multiple vulnerabilities (GLSA 202007-05) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

- [296074](#) Oracle Solaris 11.4 Support Repository Update (SRU) 22.69.4 Missing (CPUAPR2020)
- [377246](#) Alibaba Cloud Linux Security Update for libexif (ALINUX2-SA-2020:0157)
- [500291](#) Alpine Linux Security Update for libexif
- [610397](#) Google Android Devices February 2022 Security Patch Missing
- [610398](#) Google Android February 2022 Security Patch Missing for Samsung
- [610403](#) Google Android March 2022 Security Patch Missing for Huawei EMUI
- [690461](#) Free Berkeley Software Distribution (FreeBSD) Security Update for libexif (cff0b2e2-0716-11eb-9e5d-08002728f74c)

© [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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](#).

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