



# CVE-2019-7637

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-7637
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-02-08 11:29:00 UTC
<b>Updated</b>	2023-11-07 03:13:00 UTC
<b>Description</b>	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow in SDL_FillRect in

## Risk And Classification

**Problem Types: CWE-787**

## 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>	19.04	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>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Application	<a href="#">Libsdl</a>	<a href="#">Simple Directmedia Layer</a>	All	All	All	All
Application	<a href="#">Libsdl</a>	<a href="#">Simple Directmedia Layer</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All

## References

Reference	Source	Link
[security-announce] openSUSE-SU-2019:1223-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
4497 – Heap Buffer Overflow on SDL_FillRect pertaining to SDL_video	MISC	<a href="https://bugzilla.libsdl.org">bugzilla.libsdl.org</a>
USN-4143-1: SDL 2.0 vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[SECURITY] Fedora 31 Update: mingw-SDL-1.2.15-14.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
USN-4156-1: SDL vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[SECURITY] [DLA 1713-2] libsdl1.2 regression update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
USN-4156-2: SDL vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[security-announce] openSUSE-SU-2019:1633-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] Fedora 31 Update: mingw-SDL-1.2.15-14.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] [DLA 1714-2] libsdl2 regression update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] [DLA 1713-1] libsdl1.2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Vulnerabilities found in libSDL-1.2.15 and SDL2 - SDL Development - Simple Directmedia Layer	MISC	<a href="https://discourse.libsdl.org">discourse.libsdl.org</a>
[security-announce] openSUSE-SU-2019:1261-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] [DLA 2804-1] libsdl1.2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] [DLA 1714-1] libsdl2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[security-announce] openSUSE-SU-2019:1632-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[security-announce] openSUSE-SU-2019:1213-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] [DLA 2803-1] libsdl2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</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

- [178868](#) Debian Security Update for libsdl1.2 (DLA 2804-1)
- [178876](#) Debian Security Update for libsdl2 (DLA 2803-1)
- [296078](#) Oracle Solaris 11.4 Support Repository Update (SRU) 16.4.0 Missing (CPUOCT2019)
- [377229](#) Alibaba Cloud Linux Security Update for sdl (ALINUX2-SA-2020:0123)
- [500640](#) Alpine Linux Security Update for sdl
- [501246](#) Alpine Linux Security Update for sdl2
- [753165](#) SUSE Enterprise Linux Security Update for SDL (SUSE-SU-2022:14943-1)
- [940146](#) AlmaLinux Security Update for SDL (AL SA-2020:4627)

© [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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**