



# CVE-2020-14409

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

## Summary

<b>CVE</b>	CVE-2020-14409
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-19 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:17:00 UTC
<b>Description</b>	SDL (Simple DirectMedia Layer) through 2.0.12 has an Integer Overflow (and resultant SDL_memcpy heap corruption) in S

## Risk And Classification

**Problem Types:** CWE-787 | CWE-190

## 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>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Libsdl</a>	<a href="#">Simple Directmedia Layer</a>	All	All	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	-	All	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build12533	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build12658	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build12859	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build13170	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build13586	All	All
Application	<a href="#">Starwindsoftware</a>	<a href="#">Starwind Virtual San</a>	v8	build13861	All	All

## References

Reference	Source	Link
CVE-2020-14409 SDL2 vulnerability in StarWind VSAN for vSphere (VSA)	MISC	<a href="#">www.starwindsoftware</a>
[SECURITY] [DLA 3314-1] libsdl2 security update	MLIST	<a href="#">lists.debian.org</a>

SDL 2: Multiple vulnerabilities (GLSA 202107-55) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
5200 – CVE-2020-14409 and CVE-2020-14410	MISC	<a href="https://bugzilla.libSDL.org">bugzilla.libSDL.org</a>
SDL: changeset 13915:3f9b4e92c1d9	MISC	<a href="https://hg.libSDL.org">hg.libSDL.org</a>
[SECURITY] [DLA 2536-1] libSDL2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 33 Update: mingw-SDL2-2.0.12-3.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 33 Update: mingw-SDL2-2.0.12-3.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.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

<a href="#">181548</a> Debian Security Update for libSDL2 (DLA 3314-1)
<a href="#">296067</a> Oracle Solaris 11.4 Support Repository Update (SRU) 33.94.0 Missing (CPUAPR2021)
<a href="#">710040</a> Gentoo Linux SDL 2 Multiple Vulnerabilities (GLSA 202107-55)
<a href="#">751607</a> SUSE Enterprise Linux Security Update for SDL2 (SUSE-SU-2022:0104-1)
<a href="#">751616</a> OpenSUSE Security Update for SDL2 (openSUSE-SU-2022:0104-1)
<a href="#">751707</a> OpenSUSE Security Update for SDL2 (openSUSE-SU-2022:0104-2)
<a href="#">751871</a> SUSE Enterprise Linux Security Update for SDL2 (SUSE-SU-2022:0825-1)
<a href="#">752055</a> SUSE Enterprise Linux Security Update for SDL (SUSE-SU-2022:1273-1)
<a href="#">752070</a> SUSE Enterprise Linux Security Update for SDL (SUSE-SU-2022:1312-1)
<a href="#">753165</a> SUSE Enterprise Linux Security Update for SDL (SUSE-SU-2022:14943-1)

© [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](https://status.cve.report)