



CVE-2022-34568

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

Summary

CVE	CVE-2022-34568
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-28 22:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	SDL v1.2 was discovered to contain a use-after-free via the XFree function at /src/video/x11/SDL_x11yuv.c.

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libsdl	Simple Directmedia Layer	All	All	All	All

References

Reference	Source	Link	Tags
libsdl: Multiple Vulnerabilities (GLSA 202305-17) — Gentoo security	GENTOO	security.gentoo.org	
A USE AFTER FREE BUG · Issue #863 · libsdl-org/SDL-1.2 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[183356](#) Debian Security Update for libsdl1.2 (CVE-2022-34568)

[710710](#) Gentoo Linux libsdl Multiple Vulnerabilities (GLSA 202305-17)

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](#)