



CVE-2022-0496

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

Summary

CVE	CVE-2022-0496
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-29 15:15:00 UTC
Updated	2022-09-01 20:33:00 UTC
Description	A vulnerability was found in Openscad, where a DXF-format drawing with particular (not necessarily malformed!) properties

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openscad	Openscad	All	All	All	All

References

Reference	Source	Link
add safety to line lookups in DXF import, fixes #4037 · openscad/openscad@770e323 · GitHub	MISC	github.com
2050695 – (CVE-2022-0496) CVE-2022-0496 openscad: Out-of-bounds memory access in DXF loader	MISC	bugzilla.redhat.
Out-of-bounds memory access in DXF loader (path identification) · Issue #4037 · openscad/openscad · GitHub	MISC	github.com
CVE-2022-0496 Out-of-bounds memory access in DXF loader. · openscad/openscad@00a4692 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[182648](#) Debian Security Update for openscad (CVE-2022-0496)

[282589](#) Fedora Security Update for openscad (FEDORA-2022-3012e64f8c)

[20220901](#) Fedora Security Update for openscad (FEDORA-2022-1001007000)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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