



CVE-2022-0497

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

Summary

CVE	CVE-2022-0497
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 20:34:00 UTC
Description	A vulnerability was found in Openscad, where a .scad file with no trailing newline could cause an out-of-bounds read during

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	L
Out-of-bounds memory access in comment parser (file without trailing newline) · Issue #4043 · openscad/openscad · GitHub	MISC	gi
Add file bounds check to comment parser, issue #4043 by eldstal · Pull Request #4044 · openscad/openscad · GitHub	MISC	gi
2050699 – (CVE-2022-0497) CVE-2022-0497 openscad: Out-of-bounds memory access in comment parser	MISC	bi
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n'

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [181966](#) Debian Security Update for openscad (CVE-2022-0497)
- [282589](#) Fedora Security Update for openscad (FEDORA-2022-3012e64f8c)
- [282590](#) Fedora Security Update for openscad (FEDORA-2022-1961907229)

© [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](#)