



CVE-2020-28599

Published on: 02/24/2021 12:00:00 AM UTC

Last Modified on: 10/06/2022 06:48:00 PM UTC

CVE-2020-28599

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

A stack-based buffer overflow vulnerability exists in the `import_stl.cc:import_stl()` functionality of Openscad `openscad-2020.12-RC2`. A specially crafted STL file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.

CVE-2020-28599 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
OpenSCAD: Buffer overflow (GLSA 202107-35) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202107-35
[SECURITY] Fedora 33 Update: openscad-2019.05-13.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-8349f28cb9

[SECURITY] Fedora 32 Update: openscad-2019.05-13.fc32 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
text/html

 FEDORA FEDORA-2021-793da7882b

TALOS-2020-1224 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

[www.talosintelligence.com](https://www.talosintelligence.com/text/html)
text/html

 MISC
www.talosintelligence.com/vulnerability_reports/TALOS-2020-1224

TALOS-2020-1223 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

Exploit
Third Party Advisory
[talosintelligence.com](https://talosintelligence.com/text/html)
text/html

 MISC
talosintelligence.com/vulnerability_reports/TALOS-2020-1223

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[281590](#) Fedora Security Update for openscad (FEDORA-2021-8349f28cb9)

[281591](#) Fedora Security Update for openscad (FEDORA-2021-793da7882b)

[710033](#) Gentoo Linux OpenSCAD Buffer overflow (GLSA 202107-35)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Openscad	Openscad	2020.12	rc2	All	All
Application	Openscad	Openscad	2020.12	rc2	All	All
Application	Openscad	Openscad	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:

cpe:2.3:a:openscad:openscad:2020.12:rc2:*:*:*:*:

cpe:2.3:a:openscad:openscad:2020.12:rc2:*:*:*:*:

cpe:2.3:a:openscad:openscad:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)