



CVE-2020-35633

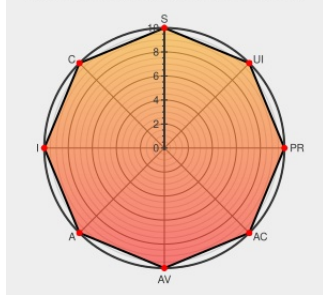
Published on: 08/30/2021 12:00:00 AM UTC

Last Modified on: 05/30/2023 06:15:00 AM UTC

CVE-2020-35633

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Computational Geometry Algorithms Library](#) from [Cgal](#) contain the following vulnerability:

A code execution vulnerability exists in the Nef polygon-parsing functionality of CGAL libcgcal CGAL-5.1.1. An oob read vulnerability exists in Nef_S2/SNC_io_parser.h SNC_io_parser<EW>::read_sface() store_sm_boundary_item() Edge_of. A specially crafted malformed file can lead to an out-of-bounds read and type confusion, which could lead to code execution. An attacker can provide malicious input to trigger this vulnerability.

CVE-2020-35633 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	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
[SECURITY] [DLA 3226-1] cgal security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20221206 [SECURITY] [DLA 3226-1] cgal security update

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

- [180656](#) Debian Security Update for cgal (CVE-2020-35633)
- [181304](#) Debian Security Update for cgal (DLA 3226-1)
- [710741](#) Gentoo Linux CGAL Multiple Vulnerabilities (GLSA 202305-34)

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cgal	Computational Geometry Algorithms Library	5.1.1	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
<code>cpe:2.3:a:cgal:computational_geometry_algorithms_library:5.1.1:***:***:***:***</code>						
<code>cpe:2.3:o:debian:debian_linux:10.0:***:***:***:***</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-35633 : A code execution vulnerability exists in the Nef polygon-parsing functionality of CGAL libcgal CGA... twitter.com/i/web/status/1...	2021-08-30 18:05:39

[← Previous ID](#)

[Next ID →](#)

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](#)