



CVE-2020-28609

Published on: Not Yet Published

Last Modified on: 01/09/2023 05:57:00 PM UTC

CVE-2020-28609

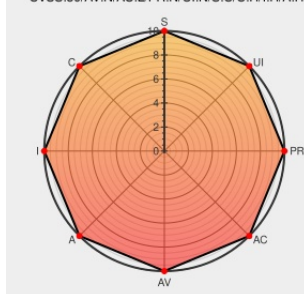
Source: Mitre

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:

Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgall CGAL-5.1.1. 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 any of these vulnerabilities. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser<PMDEC>::read_face() store_iv().

CVE-2020-28609 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [CGAL Project](#) - [libcgall](#) version = **CGAL-5.1.1**

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](#)

TALOS-2020-1225 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

[talosintelligence.com](#)
[text/html](#)

 [MISC talosintelligence.com/vulnerability_reports/TALOS-2020-1225](#)

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

[180614](#) Debian Security Update for cgal (CVE-2020-28609)

[181304](#) Debian Security Update for cgal (DLA 3226-1)

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
cpe:2.3:a:cgall:computational_geometry_algorithms_library:5.1.1:*****:						
cpe:2.3:o:debian:debian_linux:10.0:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-28609 : Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL li... twitter.com/i/web/status/1...	2022-04-18 17:05:57
 @WesUncensored	New vulnerability on the NVD: CVE-2020-28609 ift.tt/u8ivlmE	2022-04-18 18:33:14
 @workentin	New vulnerability on the NVD: CVE-2020-28609 ift.tt/u8ivlmE	2022-04-18 18:41:06

