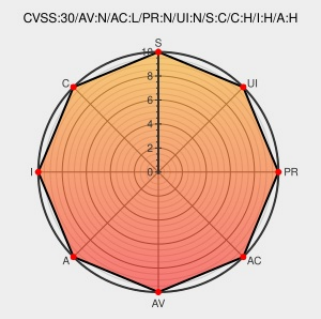
CVE-2020-28612

Published on: Not Yet Published

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

CVE-2020-28612

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



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 libcgal 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_S2/SNC_io_parser.h SNC_io_parser<EW>::read_vertex() vh->svertices_begin().

CVE-2020-28612 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **CGAL Project** - **libcgal** 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
CGAL: Multiple Vulnerabilities (GLSA 202305-34) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202305-34

Related QID Numbers

180632 Debian Security Update for cgal (CVE-2020-28612)

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

710741 Gentoo Linux CGAL Multiple Vulnerabilities (GLSA 202305-34)

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:cgal: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-2020-28612 : Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL li… twitter.com/i/web/status/1…	2022-04-18 17:07:01

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report