CVE-2020-28602

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-28602
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-18 17:15:00 UTC
Updated	2023-05-30 06:15:00 UTC
Description	Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL libcgal CGAL-5.1.1. A specia

Risk And Classification

Problem Types: CWE-129

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3226-1] cgal security update	MLIST	lists.debian.org	
TALOS-2020-1225 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	
CGAL: Multiple Vulnerabilities (GLSA 202305-34) — Gentoo security	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180727 Debian Security Update for cgal (CVE-2020-28602)

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

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