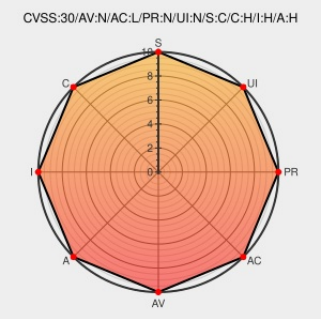
CVE-2020-28601

Published on: 03/04/2021 12:00:00 AM UTC

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

CVE-2020-28601

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



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 libcgal CGAL-5.1.1. An oob read vulnerability exists in Nef_2/PM_io_parser.h PM_io_parser::read_vertex() Face_of[] OOB read. An attacker can provide malicious input to trigger this vulnerability.

CVE-2020-28601 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	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
[SECURITY] Fedora 33 Update: CGAL-5.1.3-1.fc33 -	lists.fedoraproject.org	FEDORA FEDORA-2021-9de542ab4c

package-announce - Fedora Mailing-Lists	text/html	
[SECURITY] Fedora 34 Update: CGAL-5.2.1-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-0d42c7cb33
TALOS-2020-1225 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Technical Description Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2020-1225
[SECURITY] [DLA 2649-1] cgal security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20210505 [SECURITY] [DLA 2649-1] cgal security update
CGAL: Multiple Vulnerabilities (GLSA 202305-34) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202305-34

Related QID Numbers

178595 Debian Security Update for cgal (DLA 2649-1)

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

281708 Fedora Security Update for CGAL (FEDORA-2021-9de542ab4c)

281709 Fedora Security Update for CGAL (FEDORA-2021-0d42c7cb33)

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
Application	Cgal	Computational Geometry Algorithms Library	5.1.1	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All

cpe:2.3:a:cgal:computational_geometry_algorithms_library:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:cgal:computational_geometry_algorithms_library:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@vigilance_fr	Vigil@nce #Vulnérabilité de CGAL : quatre vulnérabilités. vigilance.fr/vulnerabilite/… Références : #CVE-2020-28601,… twitter.com/i/web/status/1…	2021-03-29 10:09:03
@vigilance_en	Vigil@nce #Vulnerability of CGAL: four vulnerabilities. vigilance.fr/vulnerability/… Identifiers: #CVE-2020-28601, #CVE-… twitter.com/i/web/status/1…	2021-03-29 10:09:04

← Previous ID

Next ID→