



# CVE-2020-28608

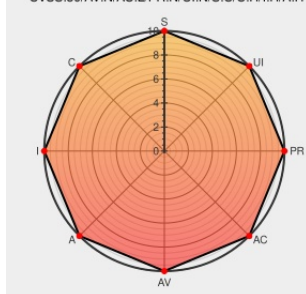
Published on: Not Yet Published

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

## CVE-2020-28608

[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\_fc().

CVE-2020-28608 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

|                                                                                       |                                                                                          |                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [SECURITY] [DLA 3226-1] cgal security update                                          | <a href="https://lists.debian.org/text/html">lists.debian.org</a><br>text/html           |  MLIST [debian-lts-announce] 20221206<br>[SECURITY] [DLA 3226-1] cgal security update                                                                   |
| TALOS-2020-1225    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | <a href="https://talosintelligence.com/text/html">talosintelligence.com</a><br>text/html |  MISC<br><a href="https://talosintelligence.com/vulnerability_reports/TALOS-2020-1225">talosintelligence.com/vulnerability_reports/TALOS-2020-1225</a> |
| CGAL: Multiple Vulnerabilities (GLSA 202305-34) — Gentoo security                     | <a href="https://security.gentoo.org/text/html">security.gentoo.org</a><br>text/html     |  GENTOO GLSA-202305-34                                                                                                                                 |

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](mailto:comment@cve.report).

Related QID Numbers

[180776](#) Debian Security Update for cgal (CVE-2020-28608)

[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                                                               | <a href="#">Cgal</a>   | <a href="#">Computational Geometry Algorithms Library</a> | 5.1.1   | All    | All     | All      |
| Operating System                                                          | <a href="#">Debian</a> | <a href="#">Debian Linux</a>                              | 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-2020-28608 : Multiple code execution vulnerabilities exists in the Nef polygon-parsing functionality of CGAL li... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-04-18 17:05:28 |
|  @WesUncensored | New vulnerability on the NVD: CVE-2020-28608 <a href="https://ift.tt/E0Tgjph">ift.tt/E0Tgjph</a>                                                                                                         | 2022-04-18 18:33:15 |
|  @workentin     | New vulnerability on the NVD: CVE-2020-28608 <a href="https://ift.tt/E0Tgjph">ift.tt/E0Tgjph</a>                                                                                                         | 2022-04-18 18:41:07 |

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)