



# CVE-2021-45342

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-45342                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2022-01-25 13:15:00 UTC                                                                                                      |
| <b>Updated</b>         | 2023-11-07 03:39:00 UTC                                                                                                      |
| <b>Description</b>     | A buffer overflow vulnerability in CDataList of the jwwlib component of LibreCAD 2.2.0-rc3 and older allows an attacker to a |

## Risk And Classification

### Problem Types: CWE-120

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                      | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 11.0    | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 34      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 35      | All    | All     | All      |
| Application      | <a href="#">Librecad</a>      | <a href="#">Librecad</a>     | 2.2.0   | alpha  | All     | All      |
| Application      | <a href="#">Librecad</a>      | <a href="#">Librecad</a>     | 2.2.0   | rc1    | All     | All      |
| Application      | <a href="#">Librecad</a>      | <a href="#">Librecad</a>     | 2.2.0   | rc2    | All     | All      |
| Application      | <a href="#">Librecad</a>      | <a href="#">Librecad</a>     | 2.2.0   | rc3    | All     | All      |
| Application      | <a href="#">Librecad</a>      | <a href="#">Librecad</a>     | All     | All    | All     | All      |

## References

| Reference                                                                                                            | Source | Link                   |
|----------------------------------------------------------------------------------------------------------------------|--------|------------------------|
| Remote Code Execution vulnerability in LibreCAD 2.2.0-rc3 (JWW CDataList) · Issue #1464 · LibreCAD/LibreCAD · GitHub | MISC   | <a href="#">github</a> |
| Debian -- Security Information -- DSA-5077-1 librecad                                                                | DEBIAN | <a href="#">www</a>    |
| [SECURITY] Fedora 35 Update: librecad-2.2.0-0.15.rc4.fc35 - package-announce - Fedora Mailing-Lists                  |        | <a href="#">list</a>   |
| [SECURITY] Fedora 34 Update: libdxfrw-1.0.1-3.fc34 - package-announce - Fedora Mailing-Lists                         | FEDORA | <a href="#">list</a>   |
| LibreCAD: Multiple Vulnerabilities (GLSA 202305-26) — Gentoo security                                                | GENTOO | <a href="#">sec</a>    |

|                                                                                                     |         |                      |
|-----------------------------------------------------------------------------------------------------|---------|----------------------|
| [SECURITY] Fedora 35 Update: librecad-2.2.0-0.15.rc4.fc35 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="#">list</a> |
| [SECURITY] Fedora 34 Update: libdxfrw-1.0.1-3.fc34 - package-announce - Fedora Mailing-Lists        |         | <a href="#">list</a> |
| CVE Program record                                                                                  | CVE.ORG | <a href="#">ww</a>   |
| NVD vulnerability detail                                                                            | NVD     | <a href="#">nvd</a>  |

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[179053](#) Debian Security Update for librecad (DLA 2908-1)

[179076](#) Debian Security Update for librecad (DSA 5077-1)

[182051](#) Debian Security Update for librecad (CVE-2021-45342)

[199313](#) Ubuntu Security Notification for LibreCAD Vulnerabilities (USN-5957-1)

[282369](#) Fedora Security Update for libdxfrw (FEDORA-2022-08d7ee21f7)

[283166](#) Fedora Security Update for libdxfrw (FEDORA-2022-3dd3274ae2)

[710732](#) Gentoo Linux LibreCAD Multiple Vulnerabilities (GLSA 202305-26)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)