



# CVE-2019-12779

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2019-12779  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2019-06-07 20:29:00 UTC   |
| <b>Updated</b>         | 2021-07-03 05:15:00 UTC   |
| <b>Description</b>     | libqb before 1.0.5 allows local users to overwrite arbitrary files via a symlink attack, because it uses predictable filenames (C |

## Risk And Classification

### Problem Types: CWE-59

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                      | Product               | Version | Update | Edition | Language |
|-------------|-----------------------------|-----------------------|---------|--------|---------|----------|
| Application | <a href="#">Clusterlabs</a> | <a href="#">Libqb</a> | All     | All    | All     | All      |
| Application | <a href="#">Clusterlabs</a> | <a href="#">Libqb</a> | All     | All    | All     | All      |

## References

| Reference  | Source  | Link                                  | Tags |
|--|---------|---------------------------------------|------|
| Release v1.0.4 · ClusterLabs/libqb · GitHub  | MISC    | <a href="#">github.com</a>            | Rele |
| Release v1.0.5 · ClusterLabs/libqb · GitHub  | MISC    | <a href="#">github.com</a>            | Rele |
| [security-announce] openSUSE-SU-2019:1752-1: moderate: Security update f                     | SUSE    | <a href="#">lists.opensuse.org</a>    |      |
| libqb: Insecure temporary file (GLSA 202107-03) — Gentoo security                            | GENTOO  | <a href="#">security.gentoo.org</a>   |      |
| 1695948 – (CVE-2019-12779) CVE-2019-12779 libqb: Insecure treatment of IPC (temporary) files | MISC    | <a href="#">bugzilla.redhat.com</a>   | E:R  |
| Insecure Temporary Files · Issue #338 · ClusterLabs/libqb · GitHub                           | MISC    | <a href="#">github.com</a>            | E:R  |
| [security-announce] openSUSE-SU-2019:1891-1: moderate: Security update f                     | SUSE    | <a href="#">lists.opensuse.org</a>    |      |
| Libqb CVE-2019-12779 Local Arbitrary File Overwrite Vulnerability                            | BID     | <a href="#">www.securityfocus.com</a> | TI   |
| [security-announce] openSUSE-SU-2019:1718-1: moderate: Security update f                     | SUSE    | <a href="#">lists.opensuse.org</a>    |      |
| Red Hat Customer Portal  | REDHAT  | <a href="#">access.redhat.com</a>     |      |
| CVE Program record   | CVE.ORG | <a href="#">www.cve.org</a>           | ca   |
| NVD vulnerability detail   | NVD     | <a href="#">nvd.nist.gov</a>          | ca   |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[377316](#) Alibaba Cloud Linux Security Update for libqb (ALINUX2-SA-2020:0080)

[710086](#) Gentoo Linux libqb Insecure temporary file vulnerability (GLSA 202107-03)

© [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](#).

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