



# CVE-2020-12803

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2020-12803   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | security@documentfoundation.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2020-06-08 16:15:00 UTC  |
| <b>Updated</b>         | 2023-12-31 14:15:00 UTC  |
| <b>Description</b>     | ODF documents can contain forms to be filled out by the user. Similar to HTML forms, the contained form data can be subn |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                     | Version | Update | Edition | Language |
|------------------|-------------------------------|-----------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>      | 31      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>      | 31      | All    | All     | All      |
| Application      | <a href="#">Libreoffice</a>   | <a href="#">Libreoffice</a> | All     | All    | All     | All      |
| Application      | <a href="#">Libreoffice</a>   | <a href="#">Libreoffice</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>      | <a href="#">Leap</a>        | 15.1    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>      | <a href="#">Leap</a>        | 15.1    | All    | All     | All      |

## References

| Reference   | Source  | Link  |
|---|---------|---|
| [SECURITY] Fedora 31 Update: libreoffice-6.3.6.2-4.fc31 - package-announcement - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| CVE-2020-12803   LibreOffice - Free Office Suite - Based on OpenOffice - Compatible with Microsoft    | MISC    | <a href="https://www.libreoffice.org">www.libreoffice.org</a>         |
| [debian-lts-announce] 20231231 [SECURITY] [DLA 3703-1] libreoffice security update                    |         | <a href="https://lists.debian.org">lists.debian.org</a>               |
| [SECURITY] Fedora 31 Update: libreoffice-6.3.6.2-4.fc31 - package-announcement - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| [security-announce] openSUSE-SU-2020:1261-1: moderate: Security update f                              | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           |
| [security-announce] openSUSE-SU-2020:1222-1: moderate: Security update f                              | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>           |
| CVE Program record  | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                         |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                       |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[199000](#) Ubuntu Security Notification for LibreOffice Vulnerabilities (USN-5694-1)

[502562](#) Alpine Linux Security Update for libreoffice

[503697](#) Alpine Linux Security Update for libreoffice

[6000415](#) Debian Security Update for libreoffice (DLA 3703-1)

[670188](#) EulerOS Security Update for libreoffice (EulerOS-SA-2021-1687)

[670883](#) EulerOS Security Update for libreoffice (EulerOS-SA-2021-1687)

[940089](#) AlmaLinux Security Update for libreoffice (ALSA-2020:4628)

[960262](#) Rocky Linux Security Update for libreoffice (RLSA-2020:4628)

© [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](#)