



CVE-2020-12802

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

Summary

CVE	CVE-2020-12802
State	PUBLIC
Assigner	security@documentfoundation.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-08 16:15:00 UTC
Updated	2023-12-31 14:15:00 UTC
Description	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote res

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	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	lists.fedoraproject.org
[debian-lts-announce] 20231231 [SECURITY] [DLA 3703-1] libreoffice security update		lists.debian.org
[SECURITY] Fedora 31 Update: libreoffice-6.3.6.2-4.fc31 - package-announcement - Fedora Mailing-Lists		lists.fedoraproject.org
CVE-2020-12802 LibreOffice - Free Office Suite - Based on OpenOffice - Compatible with Microsoft	MISC	www.libreoffice.org
[security-announce] openSUSE-SU-2020:1261-1: moderate: Security update f	SUSE	lists.opensuse.org
[security-announce] openSUSE-SU-2020:1222-1: moderate: Security update f	SUSE	lists.opensuse.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

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

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

[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](#)