



CVE-2019-9848

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

Summary

CVE	CVE-2019-9848
State	PUBLIC
Assigner	security@documentfoundation.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-17 12:15:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	LibreOffice has a feature where documents can specify that pre-installed scripts can be executed on various document eve

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link
-----------	--------	------

LibreOffice: Multiple vulnerabilities (GLSA 201908-13) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 30 Update: libreoffice-6.2.5.2-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[security-announce] openSUSE-SU-2019:2183-1: moderate: Security update f	SUSE	lists.opensuse.org
[SECURITY] Fedora 29 Update: libreoffice-6.1.6.3-3.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 29 Update: libreoffice-6.1.6.3-3.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE-2019-9848 LibreOffice - Free Office Suite - Based on OpenOffice - Compatible with Microsoft	CONFIRM	www.libreoffice.org
[SECURITY] Fedora 30 Update: libreoffice-6.2.5.2-1.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Bugtraq: [SECURITY] [DSA 4501-1] libreoffice security update	BUGTRAQ	seclists.org
[SECURITY] [DLA 1947-1] libreoffice security update	MLIST	lists.debian.org
LibreOffice Remote Code Execution and Unauthorized Access Vulnerabilities	BID	www.securityfocus.com
[security-announce] openSUSE-SU-2019:2057-1: important: Security update	SUSE	lists.opensuse.org
USN-4063-1: LibreOffice vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks to Nils Emmerich of ERNW Research GmbH for discovering and reporting this issue

Legacy QID Mappings

[356235](#) Amazon Linux Security Advisory for libreoffice : ALASLIBREOFFICE-2023-002

[377446](#) Alibaba Cloud Linux Security Update for libreoffice (ALINUX2-SA-2020:0048)

[501052](#) Alpine Linux Security Update for libreoffice

[505018](#) Alpine Linux Security Update for libreoffice

[710147](#) Gentoo Linux LibreOffice Multiple vulnerabilities (GLSA 201908-13)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report