

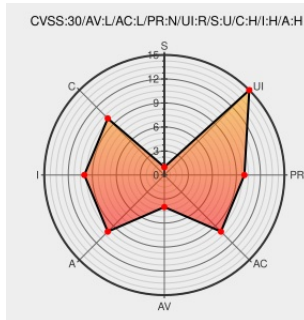


CVE-2018-10119

Published on: 04/15/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10119

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

sot/source/sdstor/stgstrms.cxx in LibreOffice before 5.4.5.1 and 6.x before 6.0.1.1 uses an incorrect integer data type in the StgSmallStrm class, which allows remote attackers to cause a denial of service (use-after-free with write access) or possibly have unspecified other impact via a crafted document that uses the structured storage ole2 wrapper file format.

CVE-2018-10119 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Gerrit Code Review	Patch Vendor Advisory	MISC gerrit.libreoffice.org/#/c/48756/

	gerrit.libreoffice.org text/html	
fdd41c995d1f719e92c6f083e780226114762f05 - core - Gitiles	Patch Vendor Advisory gerrit.libreoffice.org text/html	 MISC gerrit.libreoffice.org/gitweb?p=core.git;a=commit;h=fdd41c995d1f719e92c6f083e780226114762f05
Gerrit Code Review	Patch Vendor Advisory gerrit.libreoffice.org text/html	 MISC gerrit.libreoffice.org/#/c/48751/
Debian -- Security Information -- DSA-4178-1 libreoffice	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4178
Gerrit Code Review	Patch Vendor Advisory gerrit.libreoffice.org text/html	 MISC gerrit.libreoffice.org/#/c/48757/
Gerrit Code Review	Patch Vendor Advisory gerrit.libreoffice.org text/html	 MISC gerrit.libreoffice.org/#/c/48758/
5747 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	Third Party Advisory bugs.chromium.org text/html	 MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=5747
USN-3883-1: LibreOffice vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3883-1
CVE-2018-10119 LibreOffice - Free Office Suite - Fun Project - Fantastic People	Vendor Advisory www.libreoffice.org text/html	 MISC www.libreoffice.org/about-us/security/advisories/cve-2018-10119/
[SECURITY] [DLA 1356-1] libreoffice security update	Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20180419 [SECURITY] [DLA 1356-1] libreoffice security update
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2018:3054

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating	Canonical	Ubuntu Linux	16.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:						
cpe:2.3:o:debian:debian_linux:7.0:***:***:***:						
cpe:2.3:o:debian:debian_linux:8.0:***:***:***:						
cpe:2.3:o:debian:debian_linux:9.0:***:***:***:						
cpe:2.3:o:debian:debian_linux:7.0:***:***:***:						
cpe:2.3:o:debian:debian_linux:8.0:***:***:***:						

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:
cpe:2.3:a:libreoffice:libreoffice:*:*:*:*:*:
cpe:2.3:a:libreoffice:libreoffice:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)