



CVE-2015-5212

Published on: 11/10/2015 12:00:00 AM UTC

Last Modified on: 02/07/2022 04:29:00 PM UTC

CVE-2015-5212

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

Certain versions of [Openoffice](#) from [Apache](#) contain the following vulnerability:

Integer underflow in LibreOffice before 4.4.5 and Apache OpenOffice before 4.1.2, when the configuration setting "Load printer settings with the document" is enabled, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via crafted PrinterSetup data in an ODF document.

CVE-2015-5212 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

CVE-2015-5212 | LibreOffice - Free Office Suite - Fun Project - Fantastic People

[Vendor Advisory](#)
www.libreoffice.org
[text/html](#)

[CONFIRM www.libreoffice.org/about-us/security/advisories/cve-2015-5212/](http://www.libreoffice.org/about-us/security/advisories/cve-2015-5212/)

LibreOffice, OpenOffice: Multiple vulnerabilities (GLSA 201611-03) — Gentoo security

security.gentoo.org
[text/html](#)

[GENTOO GLSA-201611-03](#)

CVE-2015-5212

[Vendor Advisory](#)
www.openoffice.org
[text/html](#)

[CONFIRM www.openoffice.org/security/cves/CVE-2015-5212.html](http://www.openoffice.org/security/cves/CVE-2015-5212.html)

LibreOffice Multiple Remote Code Execution and Information Disclosure Vulnerabilities

[cve.report \(archive\)](#)
[text/html](#)

[BID 77486](#)

Debian -- Security Information -- DSA-3394-1 libreoffice	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3394
Apache OpenOffice Bugs Let Remote Users Obtain Files and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTRACK 1034091
LibreOffice Bugs Let Remote Users Obtain Files and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTRACK 1034085
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:2619
LibreOffice, OpenOffice: Multiple vulnerabilities (GLSA 201603-05) — Gentoo Security	security.gentoo.org text/html	 GENTOO GLSA-201603-05
Oracle Linux Bulletin - October 2015	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinoct2015-2719645.html
USN-2793-1: LibreOffice vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2793-1

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
Application	Apache	Openoffice	All	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	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	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
cpe:2.3:a:apache:openoffice:*.***.***.***:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*.***:lts:*.***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*.***:lts:*.***:						
cpe:2.3:o:canonical:ubuntu_linux:15.04:*.***.***.***:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*.***:lts:*.***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*.***:lts:*.***:						
cpe:2.3:o:canonical:ubuntu_linux:15.04:*.***.***.***:						
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:7.0:*.***.***.***:						
cpe:2.3:o:debian:debian_linux:8.0:*.***.***.***:						
cpe:2.3:a:libreoffice:libreoffice:*.***.***.***:						

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