



CVE-2011-2685

Published on: 07/21/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:20 PM UTC

CVE-2011-2685

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

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

Stack-based buffer overflow in the Lotus Word Pro import filter in LibreOffice before 3.3.3 allows remote attackers to execute arbitrary code via a crafted .lwp file.

CVE-2011-2685 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

oss-security - Re: libreoffice/openoffice.org CVE id request

www.openwall.com
text/html

[MLIST \[oss-security\] 20110712 Re: libreoffice/openoffice.org CVE id request](#)

openSUSE-SU-2011:1143-2: moderate: libreoffice to 3.4

lists.opensuse.org
text/html

[SUSE openSUSE-SU-2011:1143](#)

US-CERT Vulnerability Note VU#953183 - LibreOffice 3.3 'Lotus Word Pro' document import filter contains multiple vulnerabilities

[Patch](#)
[US Government Resource](#)
www.kb.cert.org
text/html

[CERT-VN VU#953183](#)

libreoffice/filters - obsolete from 3.5 - Import and export filters

[Patch](#)
cgit.freedesktop.org
text/html

[MISC](#)
cgit.freedesktop.org/libreoffice/filters/commit/?id=d93fa011d713100775cd3ac88c468b6830d48877

libreoffice/filters - obsolete from 3.5 - Import and export filters

[Patch](#)
cgit.freedesktop.org

[MISC](#)
cgit.freedesktop.org/libreoffice/filters/commit/?id=d93fa011d713100775cd3ac88c468b6830d48877

[text/html](#)

id=278831e37a23e9e2e29ca811c3a5398b7c67464d

oss-security - libreoffice/openoffice.org CVE id request

[www.openwall.com](#)[text/html](#) MLIST [oss-security] 20110706
libreoffice/openoffice.org CVE id requestSupport / Security / Advisories // MDVSA-2011:172 |
Mandriva[www.mandriva.com](#)[text/html](#) MANDRIVA MDVSA-2011:172

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	Libreoffice	Libreoffice	3.3.0	All	All	All
Application	Libreoffice	Libreoffice	3.3.1	All	All	All
Application	Libreoffice	Libreoffice	3.3.0	All	All	All
Application	Libreoffice	Libreoffice	3.3.1	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
cpe:2.3:a:libreoffice:libreoffice:3.3.0:*:*:*:*:*:						
cpe:2.3:a:libreoffice:libreoffice:3.3.1:*:*:*:*:*:						
cpe:2.3:a:libreoffice:libreoffice:3.3.0:*:*:*:*:*:						
cpe:2.3:a:libreoffice:libreoffice:3.3.1:*:*:*:*:*:						
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](#)