



CVE-2012-1149

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

Summary

CVE	CVE-2012-1149
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-21 15:55:00 UTC
Updated	2023-02-13 00:23:00 UTC
Description	Integer overflow in the vclmi.dll module in OpenOffice.org (OOo) 3.3, 3.4 Beta, and possibly earlier, and LibreOffice before :

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Openoffice.org	3.3.0	All	All	All
Application	Apache	Openoffice.org	3.4	beta	All	All
Application	Apache	Openoffice.org	3.3.0	All	All	All
Application	Apache	Openoffice.org	3.4	beta	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	15	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Fedoraproject	Fedora	15	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Application	Libreoffice	Libreoffice	All	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.2.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.2.z	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References

Reference

[Security Alerts - Secunia](#)

[Security Advisory SA47244 - LibreOffice Integer Overflow Vulnerabilities - Secunia](#)

[CVE-2012-1149 » LibreOffice](#)

[CVE-2012-1149 - Red Hat Customer Portal](#)

81988

[Security Advisory SA49140 - Debian update for openoffice.org - Secunia](#)

[Security Advisory SA60799 - Gentoo openoffice Multiple Vulnerabilities - Secunia](#)

[Malformed Request](#)

[Security Alerts - Secunia](#)

[Red Hat Customer Portal](#)

[Support / Security / Advisories // MDVSA-2012:090 | Mandriva](#)

[\[SECURITY\] Fedora 16 Update: libreoffice-3.4.5.2-15.fc16](#)

[Support / Security / Advisories // MDVSA-2012:091 | Mandriva](#)

[Gentoo Linux Documentation -- LibreOffice: Multiple vulnerabilities](#)

[821726 – \(CVE-2012-1149\) CVE-2012-1149 openoffice.org, libreoffice: Integer overflows, leading to heap-buffer overflows in JPEG, PNG and](#)

[NEOHAPSIS - Peace of Mind Through Integrity and Insight](#)

[Security Advisory SA46992 - OpenOffice.org Documents Processing Multiple Vulnerabilities - Secunia](#)

[Gentoo Linux Documentation -- OpenOffice, LibreOffice: Multiple vulnerabilities](#)

[Red Hat Customer Portal](#)

[OpenOffice.org Integer Overflow in 'vclmi.dll' Lets Remote Users Execute Arbitrary Code - SecurityTracker](#)

[Debian -- Security Information -- DSA-2487-1 openoffice.org](#)

[Security Alerts - Secunia](#)

IBM X-Force Exchange

Debian -- Security Information -- DSA-2473-1 openoffice.org

[SECURITY] Fedora 15 Update: libreoffice-3.3.4.1-5.fc15

CVE-2012-1149

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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/cve). This site includes MITRE data granted under the following [license](#).

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