



CVE-2006-5870

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-5870
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-31 05:00:00 UTC
Updated	2018-10-17 21:45:00 UTC
Description	Multiple integer overflows in OpenOffice.org (OOo) 2.0.4 and earlier, and possibly other versions before 2.1.0; and StarOffice

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openoffice	Openoffice	All	All	All	All
Application	Sun	Staroffice	6.0	All	All	All
Application	Sun	Staroffice	7.0	All	All	All
Application	Sun	Staroffice	8.0	All	All	All
Application	Sun	Staroffice	6.0	All	All	All
Application	Sun	Staroffice	7.0	All	All	All
Application	Sun	Staroffice	8.0	All	All	All

References

Reference

[SecurityFocus](#)

[SGI Advanced Linux Environment Multiple Updates - Secunia Advisories - Vulnerability Intelligence - Secunia.com](#)

[Search by bug number](#)

[Repository / Oval Repository](#)

[OpenOffice.org Office Suite Integer Overflow in Processing WMF/EMF Files Lets Remote Users Execute Arbitrary Code - SecurityTracker](#)

[\[SECURITY\] Fedora Core 6 Update: openoffice.org-2.0.4-5.5.10 | FedoraNEWS.ORG](#)

[Gentoo Linux Documentation -- OpenOffice.org: EMF/WMF file handling vulnerabilities](#)

#102735: Security Vulnerability With StarOffice/StarSuite Versions 6, 7 and 8 Related to the '.wmf' File Format

Red Hat update for openoffice.org - Advisories - Secunia

32610

StarOffice WMF/EMF Processing Buffer Overflow Vulnerabilities - Advisories - Secunia

OpenOffice.org Files

Webmail- OVH

SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: OpenOffice_org WMF buffer overflows (SUSE-SA:2

Ubuntu update for openoffice.org - Advisories - Secunia

issues.rpath.com/browse/RPL-905

Fedora update for openoffice.org - Advisories - Secunia

SecurityFocus

OpenOffice WMF/EMF Processing Buffer Overflow Vulnerabilities - Advisories - Secunia

USN-406-1: OpenOffice.org vulnerability | Ubuntu

Advisories - Mandriva Linux

Gentoo update for openoffice - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

32611

SecurityFocus

Advisories - Research - Next Generation Security Software

rPath update for openoffice.org - Advisories - Secunia

SecurityFocus

Mandriva update for OpenOffice.org - Advisories - Secunia

Repository / Oval Repository

Debian update for openoffice.org - Advisories - Secunia

IBM X-Force Exchange

Debian -- Security Information -- DSA-1246-1 openoffice.org

US-CERT Vulnerability Note VU#220288

SUSE update for OpenOffice_org - Advisories - Secunia

SecurityFocus

rhn.redhat.com | Red Hat Support

20070101-01-P

20070104 High Risk Vulnerability in the OpenOffice and StarOffice Suites

CVE Program record

NVD vulnerability detail



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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

© [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](#) 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](#)