



CVE-2007-2834

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

Summary

CVE	CVE-2007-2834
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-18 21:17:00 UTC
Updated	2022-02-07 17:16:00 UTC
Description	Integer overflow in the TIFF parser in OpenOffice.org (OOo) before 2.3; and Sun StarOffice 6, 7, and 8 Office Suite (StarSu

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Openoffice	All	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	alpha	All
Operating System	Debian	Debian Linux	3.1	All	amd64	All
Operating System	Debian	Debian Linux	3.1	All	arm	All
Operating System	Debian	Debian Linux	3.1	All	hppa	All
Operating System	Debian	Debian Linux	3.1	All	ia-32	All
Operating System	Debian	Debian Linux	3.1	All	ia-64	All
Operating System	Debian	Debian Linux	3.1	All	m68k	All
Operating System	Debian	Debian Linux	3.1	All	mips	All
Operating System	Debian	Debian Linux	3.1	All	mipsel	All
Operating System	Debian	Debian Linux	3.1	All	ppc	All
Operating System	Debian	Debian Linux	3.1	All	s-390	All
Operating System	Debian	Debian Linux	3.1	All	sparc	All

Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	alpha	All
Operating System	Debian	Debian Linux	4.0	All	amd64	All
Operating System	Debian	Debian Linux	4.0	All	arm	All
Operating System	Debian	Debian Linux	4.0	All	hppa	All
Operating System	Debian	Debian Linux	4.0	All	ia-32	All
Operating System	Debian	Debian Linux	4.0	All	ia-64	All
Operating System	Debian	Debian Linux	4.0	All	m68k	All
Operating System	Debian	Debian Linux	4.0	All	mips	All
Operating System	Debian	Debian Linux	4.0	All	mipsel	All
Operating System	Debian	Debian Linux	4.0	All	powerpc	All
Operating System	Debian	Debian Linux	4.0	All	s-390	All
Operating System	Debian	Debian Linux	4.0	All	sparc	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	alpha	All
Operating System	Debian	Debian Linux	3.1	All	amd64	All
Operating System	Debian	Debian Linux	3.1	All	arm	All
Operating System	Debian	Debian Linux	3.1	All	hppa	All
Operating System	Debian	Debian Linux	3.1	All	ia-32	All
Operating System	Debian	Debian Linux	3.1	All	ia-64	All
Operating System	Debian	Debian Linux	3.1	All	m68k	All
Operating System	Debian	Debian Linux	3.1	All	mips	All
Operating System	Debian	Debian Linux	3.1	All	mipsel	All
Operating System	Debian	Debian Linux	3.1	All	ppc	All
Operating System	Debian	Debian Linux	3.1	All	s-390	All
Operating System	Debian	Debian Linux	3.1	All	sparc	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	alpha	All
Operating System	Debian	Debian Linux	4.0	All	amd64	All
Operating System	Debian	Debian Linux	4.0	All	arm	All
Operating System	Debian	Debian Linux	4.0	All	hppa	All
Operating System	Debian	Debian Linux	4.0	All	ia-32	All
Operating System	Debian	Debian Linux	4.0	All	ia-64	All
Operating System	Debian	Debian Linux	4.0	All	m68k	All
Operating System	Debian	Debian Linux	4.0	All	mips	All

Operating System	Debian	Debian Linux	4.0	All	mipsel	All
Operating System	Debian	Debian Linux	4.0	All	powerpc	All
Operating System	Debian	Debian Linux	4.0	All	s-390	All
Operating System	Debian	Debian Linux	4.0	All	sparc	All
Operating System	Fedoraproject	Fedora Core	3	All	All	All
Operating System	Fedoraproject	Fedora Core	6	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Application	Openoffice	Openoffice	1.1.3	All	All	All
Application	Openoffice	Openoffice	2.0.4	All	All	All
Application	Openoffice	Openoffice	2.2.1	All	All	All
Application	Openoffice	Openoffice	1.1.3	All	All	All
Application	Openoffice	Openoffice	2.0.4	All	All	All
Application	Openoffice	Openoffice	2.2.1	All	All	All
Operating System	Redhat	Enterprise Linux	3.0	All	as	All
Operating System	Redhat	Enterprise Linux	3.0	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	ws	All
Operating System	Redhat	Enterprise Linux	4.0	All	as	All
Operating System	Redhat	Enterprise Linux	4.0	All	es	All
Operating System	Redhat	Enterprise Linux	4.0	All	ws	All
Operating System	Redhat	Enterprise Linux	5.0	All	client	All
Operating System	Redhat	Enterprise Linux	3.0	All	as	All
Operating System	Redhat	Enterprise Linux	3.0	All	es	All
Operating System	Redhat	Enterprise Linux	3.0	All	ws	All
Operating System	Redhat	Enterprise Linux	4.0	All	as	All
Operating System	Redhat	Enterprise Linux	4.0	All	es	All
Operating System	Redhat	Enterprise Linux	4.0	All	ws	All
Operating System	Redhat	Enterprise Linux	5.0	All	client	All
Operating System	Redhat	Fedora Core	3	All	All	All
Operating System	Redhat	Fedora Core	3	All	All	All
Operating System	Redhat	Fedora Core	6	All	All	All
Operating System	Redhat	Fedora Core	6	All	All	All
Operating System	Redhat	Linux	3.0	All	desktop	All
Operating System	Redhat	Linux	4.0	All	desktop	All
Operating System	Redhat	Linux	3.0	All	desktop	All

Operating System	Hedhat	Linux	4.0	All	desktop	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
Application	Sun	Starsuite	All	All	All	All
Application	Sun	Starsuite	All	All	All	All
Operating System	Ubuntu	Ubuntu Linux	5.04	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	5.04	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	5.04	All	powerpc	All
Operating System	Ubuntu	Ubuntu Linux	5.04	All	amd64	All
Operating System	Ubuntu	Ubuntu Linux	5.04	All	i386	All
Operating System	Ubuntu	Ubuntu Linux	5.04	All	powerpc	All

References

Reference

[OpenOffice TIFF File Parser Multiple Integer Overflow Vulnerabilities](#)

[IBM X-Force Exchange](#)

[OpenOffice TIFF Parsing Integer Overflow Vulnerabilities - Advisories - Secunia](#)

[Debian update for openoffice.org - Advisories - Secunia](#)

[#102994: Manipulated TIFF Files or Documents Containing Manipulated TIFF Files May Lead to Heap Overflows and Arbitrary Code Execution](#)

[20070917 Multiple Vendor OpenOffice TIFF File Parsing Multiple Integer Overflow Vulnerabilities](#)

[Gentoo update for openoffice - Advisories - Secunia](#)

[Repository / Oval Repository](#)

[Fedora update for openoffice.org - Advisories - Secunia](#)

[OpenOffice 2 TIFF Parsing Integer Overflow Vulnerabilities - Advisories - Secunia](#)

[Gentoo Bug 192818 - app-office/openoffice{,-bin}: Manipulated TIFF files can lead to heap overflows and arbitrary code execution \(CVE-2007-0917\)](#)

[SUSE update for OpenOffice_org - Advisories - Secunia](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[issues.rpath.com/browse/RPL-1740](#)

[Ubuntu update for openoffice.org - Advisories - Secunia](#)

[USN-524-1: OpenOffice.org vulnerability | Ubuntu](#)

[Fedora update for openoffice.org - Advisories - Secunia](#)

[Support](#)

200190

Mandriva update for openoffice.org - Advisories - Secunia

Debian -- Security Information -- DSA-1375-1 openoffice.org

404 Not Found

Red Hat update for openoffice.org - Advisories - Secunia

SecurityFocus

OpenOffice Buffer Overflow in Processing TIFF Images Lets Remote Users Execute Arbitrary Code - SecurityTracker

Sun StarOffice Office Suite TIFF Parsing Integer Overflow Vulnerabilities - Advisories - Secunia

[security-announce] SUSE Security Announcement: OpenOffice_org TIFF prob

404 Not Found

rPath update for openoffice.org - Advisories - Secunia

Gentoo Linux Documentation -- OpenOffice.org: Heap-based buffer overflow

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Advisories - Mandriva Linux

CVE-2007-02834

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](https://www.mitre.org/licenses).

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