



# CVE-2009-0201

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2009-0201
<b>State</b>	PUBLIC
<b>Assigner</b>	PSIRT-CNA@flexerasoftware.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-09-02 17:30:00 UTC
<b>Updated</b>	2018-10-11 21:00:00 UTC
<b>Description</b>	Heap-based buffer overflow in OpenOffice.org (OOo) before 3.1.1 and StarOffice/StarSuite 7, 8, and 9 might allow remote e

## Risk And Classification

**Problem Types: CWE-119**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	1.1.2	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	1.1.3	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	1.1.4	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	1.1.5	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.0	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.0.2	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.0.3	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.0.4	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.1	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.2	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.2.1	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.3	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.3.1	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.4	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.4.1	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.4.1	All	64-bit	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	1.1.2	All	All	All

Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	1.1.3	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	1.1.4	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	1.1.5	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.0	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.0.2	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.0.3	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.0.4	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.1	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.2	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.2.1	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.3	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.3.1	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.4	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.4.1	All	All	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	2.4.1	All	64-bit	All
Application	<a href="#">Openoffice</a>	<a href="#">Openoffice.org</a>	All	All	All	All

## References

Reference	Source	Link
OpenOffice.org Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	<a href="#">secun</a>
SecurityTracker.com Archives - OpenOffice Table Parsing Buffer Overflow Lets Remote Users Execute Arbitrary Code	SECTRACK	<a href="#">www.</a>
1020715	SUNALERT	<a href="#">sunsc</a>
263508	SUNALERT	<a href="#">sunsc</a>
development: 3.1.1 (build OOO310_m19) - Release Notes	MISC	<a href="#">devel</a>
Debian -- Security Information -- DSA-1880-1 openoffice.org	DEBIAN	<a href="#">www.</a>
Security Advisory SA60799 - Gentoo openoffice Multiple Vulnerabilities - Secunia	SECUNIA	<a href="#">secun</a>
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:015	SUSE	<a href="#">lists.o</a>
OpenOffice Word Document Table Parsing Multiple Heap Based Buffer Overflow Vulnerabilities	BID	<a href="#">www.</a>
SecurityFocus	BUGTRAQ	<a href="#">www.</a>
Gentoo Linux Documentation -- OpenOffice, LibreOffice: Multiple vulnerabilities	GENTOO	<a href="#">www.</a>
CVE-2009-0200 / CVE-2009-0201	CONFIRM	<a href="#">www.</a>
Support / Security / Advisories // MDVSA-2010:105   Mandriva	MANDRIVA	<a href="#">www.</a>
Repository / Oval Repository	OVAL	<a href="#">oval.c</a>
Support / Security / Advisories // MDVSA-2010:035   Mandriva	MANDRIVA	<a href="#">www.</a>
Vulnerabilities - Secunia Research - Vulnerability Information - Secunia.com	MISC	<a href="#">secun</a>
OpenOffice.org Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	MANDRIVA	

Support / Security / Advisories // MDVSA-2010:091   Mandriva	MANDRIVA	<a href="#">www.mandriva.com</a>
Security Advisory SA36750 - Sun StarOffice / StarSuite Word Document Table Parsing Vulnerabilities - Secunia	SECUNIA	<a href="#">secunia.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.vupen.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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](#)