



CVE-2009-2139

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

Summary

CVE	CVE-2009-2139
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-09-08 23:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Heap-based buffer overflow in svtools/source/filter.vcl/wmf/enhwmf.cxx in Go-oo 2.x and 3.x before 3.0.1, previously named

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sun	Openoffice.org	2.0.0	All	All	All

Application	Sun	Openoffice.org	2.0.3	All	All	All
Application	Sun	Openoffice.org	2.0.4	All	All	All
Application	Sun	Openoffice.org	2.1.0	All	All	All
Application	Sun	Openoffice.org	2.2.0	All	All	All
Application	Sun	Openoffice.org	2.2.1	All	All	All
Application	Sun	Openoffice.org	2.3.0	All	All	All
Application	Sun	Openoffice.org	2.3.1	All	All	All
Application	Sun	Openoffice.org	2.4.0	All	All	All
Application	Sun	Openoffice.org	2.4.1	All	All	All
Application	Sun	Openoffice.org	2.4.2	All	All	All
Application	Sun	Openoffice.org	2.4.3	All	All	All
Application	Sun	Openoffice.org	3.0.0	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References	
Reference	Source
Debian update for openoffice.org - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91ae-364da2661108
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:015	af854a3a-2127-422b-91ae-364da2661108
OpenOffice EMF File Parser Remote Command Execution Vulnerability	af854a3a-2127-422b-91ae-364da2661108
cgit.freedesktop.org/ooo-build/ooo-build/commit	af854a3a-2127-422b-91ae-364da2661108
Support / Security / Advisories / / MDVSA-2010:105 Mandriva	af854a3a-2127-422b-91ae-364da2661108
'Re: [oss-security] OpenOffice.org CVE-2009-2139' - MARC	af854a3a-2127-422b-91ae-364da2661108
oss-security - Re: CVE-2009-3239 is a duplicate of CVE-2009-2139 and CVE-2009-2140	af854a3a-2127-422b-91ae-364da2661108
'Re: [oss-security] OpenOffice.org CVE-2009-2139' - MARC	af854a3a-2127-422b-91ae-364da2661108
Support / Security / Advisories / / MDVSA-2010:035 Mandriva	af854a3a-2127-422b-91ae-364da2661108
Support / Security / Advisories / / MDVSA-2010:091 Mandriva	af854a3a-2127-422b-91ae-364da2661108
'Re: [oss-security] OpenOffice.org CVE-2009-2139' - MARC	af854a3a-2127-422b-91ae-364da2661108
Debian -- Security Information -- DSA-1880-1 openoffice.org	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Debian	2009-09-10	Torsten Kluge	Message ID: 20090910140000.10000@torstenkluge.net From: Torsten Kluge <torsten.kluge@torstenkluge.net> To: "OpenOffice.org Security" <openoffice-security@openoffice.org> Subject: OpenOffice.org CVE-2009-2139

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)