



CVE-2009-1962

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

Summary

CVE	CVE-2009-1962
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-08 01:00:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	Xfig, possibly 3.2.5, allows local users to read and write arbitrary files via a symlink attack on the (1) xfig-eps[PID], (2) xfig-p

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	4.0	All	s/390	All
Operating System	Debian	Debian Linux	5.0	All	alpha	All
Operating System	Debian	Debian Linux	5.0	All	amd64	All
Operating System	Debian	Debian Linux	5.0	All	arm	All
Operating System	Debian	Debian Linux	5.0	All	armel	All

Operating System	Debian	Debian Linux	5.0	All	hppa	All
Operating System	Debian	Debian Linux	5.0	All	ia-32	All
Operating System	Debian	Debian Linux	5.0	All	ia-64	All
Operating System	Debian	Debian Linux	5.0	All	m68k	All
Operating System	Debian	Debian Linux	5.0	All	mips	All
Operating System	Debian	Debian Linux	5.0	All	mipsel	All
Operating System	Debian	Debian Linux	5.0	All	powerpc	All
Operating System	Debian	Debian Linux	5.0	All	s/390	All
Operating System	Debian	Debian Linux	5.0	All	sparc	All
Operating System	Debian	Debian Linux	5.0	All	s/390	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	sparc	All
Operating System	Debian	Debian Linux	4.0	All	s/390	All
Operating System	Debian	Debian Linux	5.0	All	alpha	All
Operating System	Debian	Debian Linux	5.0	All	amd64	All
Operating System	Debian	Debian Linux	5.0	All	arm	All
Operating System	Debian	Debian Linux	5.0	All	armel	All
Operating System	Debian	Debian Linux	5.0	All	hppa	All
Operating System	Debian	Debian Linux	5.0	All	ia-32	All
Operating System	Debian	Debian Linux	5.0	All	ia-64	All
Operating System	Debian	Debian Linux	5.0	All	m68k	All
Operating System	Debian	Debian Linux	5.0	All	mips	All
Operating System	Debian	Debian Linux	5.0	All	mipsel	All
Operating System	Debian	Debian Linux	5.0	All	powerpc	All
Operating System	Debian	Debian Linux	5.0	All	sparc	All
Operating System	Debian	Debian Linux	5.0	All	s/390	All

Application	Xfig	Xfig	3.2.5	All	All	All
Application	Xfig	Xfig	3.2.5	All	All	All
References						
Reference			Source	Link	Tags	
IBM X-Force Exchange			XF	exchange.xforce.ibmcloud.com		
Support / Security / Advisories / / MDVSA-2009:244 Mandriva			MANDRIVA	www.mandriva.com		
Xfig Multiple Insecure Temporary File Creation Vulnerabilities			BID	www.securityfocus.com		
oss-security - CVE id request: xfig insecure tmp files			MLIST	www.openwall.com		
Xfig Insecure Temporary Files - Secunia.com			SECUNIA	secunia.com		
CVE Program record			CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail			NVD	nvd.nist.gov	canonical, analysis	
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](#).

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

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