



CVE-2006-2449

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

Summary

CVE	CVE-2006-2449
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-15 10:02:00 UTC
Updated	2018-10-18 16:40:00 UTC
Description	KDE Display Manager (KDM) in KDE 3.2.0 up to 3.5.3 allows local users to read arbitrary files via a symlink attack related to

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Kde	Kde	3.2	All	All	All
Operating System	Kde	Kde	3.2.1	All	All	All
Operating System	Kde	Kde	3.2.2	All	All	All
Operating System	Kde	Kde	3.2.3	All	All	All
Operating System	Kde	Kde	3.3	All	All	All
Operating System	Kde	Kde	3.3.1	All	All	All
Operating System	Kde	Kde	3.3.2	All	All	All
Operating System	Kde	Kde	3.4	All	All	All
Operating System	Kde	Kde	3.4.1	All	All	All
Operating System	Kde	Kde	3.4.2	All	All	All
Operating System	Kde	Kde	3.4.3	All	All	All
Operating System	Kde	Kde	3.5	All	All	All
Operating System	Kde	Kde	3.5.2	All	All	All
Operating System	Kde	Kde	3.5.3	All	All	All
Operating System	Kde	Kde	3.2	All	All	All
Operating System	Kde	Kde	3.2.1	All	All	All
Operating System	Kde	Kde	3.2.2	All	All	All

Operating System	Kde	Kde	3.2.3	All	All	All
Operating System	Kde	Kde	3.3	All	All	All
Operating System	Kde	Kde	3.3.1	All	All	All
Operating System	Kde	Kde	3.3.2	All	All	All
Operating System	Kde	Kde	3.4	All	All	All
Operating System	Kde	Kde	3.4.1	All	All	All
Operating System	Kde	Kde	3.4.2	All	All	All
Operating System	Kde	Kde	3.4.3	All	All	All
Operating System	Kde	Kde	3.5	All	All	All
Operating System	Kde	Kde	3.5.2	All	All	All
Operating System	Kde	Kde	3.5.3	All	All	All

References						
Reference			Source		Link	
KDE KDM Session Type Symbolic Link Vulnerability			BID		www.securityfocus.com	
Gentoo Linux Documentation -- KDM: Symlink vulnerability			GENTOO		www.gentoo.org	
Secunia - Advisories - Slackware update for kdbase			SECUNIA		secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN		www.vupen.com	
IBM X-Force Exchange			XF		exchange.xforce.ibmcloud.com	
rhn.redhat.com Red Hat Support			REDHAT		www.redhat.com	
www.kde.org/info/security/advisory-20060614-1.txt			CONFIRM		www.kde.org	
Debian -- Security Information -- DSA-1156-1 kdbase			DEBIAN		www.debian.org	
KDE KDM Arbitrary File Reading Vulnerability - Advisories - Secunia			SECUNIA		secunia.com	
Debian update for kdbase - Secunia Advisories - Vulnerability Intelligence - Secunia.com			SECUNIA		secunia.com	
Red Hat update for kdbase - Advisories - Secunia			SECUNIA		secunia.com	
Advisories - Mandriva Linux			MANDRIVA		www.mandriva.com	
Secunia - Advisories - Gentoo update for kdbase / KDM			SECUNIA		secunia.com	
Advisories - Mandriva Linux			MANDRIVA		www.mandriva.com	
26511			OSVDB		www.osvdb.org	
SecurityTracker.com Archives - KDE KDM Symlink Bug Lets Local Users View Files			SECTRACK		securitytracker.com	
SecurityFocus			BUGTRAQ		www.securityfocus.com	
SecurityFocus			BUGTRAQ		www.securityfocus.com	
Ubuntu update for kdm - Advisories - Secunia			SECUNIA		secunia.com	
The Slackware Linux Project: Slackware Security Advisories			SLACKWARE		slackware.com	
Secunia - Advisories - SUSE update for kdbase3-kdm			SECUNIA		secunia.com	
KDE 3.5.3 Security Update: KDM Arbitrary File Reading Vulnerability			UBUNTU		ubuntu.com	

USN-301-1: kdm vulnerability Ubuntu security notices	UBUNTU	usn.ubuntu.com
Security Announcement	SUSE	www.novell.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
Secunia - Advisories - Mandriva update for kdebase	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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/cve).

Free CVE JSON API cve.report/api

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