



CVE-2004-1171

Published on: 12/10/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1171

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Kde](#) from [Kde](#) contain the following vulnerability:

KDE 3.2.x and 3.3.0 through 3.3.2, when saving credentials that are (1) manually entered by the user or (2) created by the SMB protocol handler, stores those credentials for plaintext in the user's .desktop file, which may be created with world-readable permissions, which could allow local users to obtain usernames and passwords for remote resources such as SMB shares.

CVE-2004-1171 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

Secunia - Advisories - Fedora update for kdbase/kdelibs

[web.archive.org](#)
[text/html](#)

[X](#) SECUNIA 13486

SecurityTracker.com Archives - KDE May Disclose SMB Passwords to Remote Users Via URLs

[securitytracker.com](#)
[text/html](#)

[G](#) SECTRAK 1012471

P-051: SMB Password Disclosure

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[G](#) CIAC P-051

'KDE Security Advisory: plain text password exposure' - MARC

[marc.info](#)
[text/html](#)

[G](#) BUGTRAQ 20041209 KDE Security Advisory: plain text password exposure

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[G](#) XF kde-smb-password-plaintext(18267)

US-CERT Vulnerability Note VU#305294	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#305294
Secunia - Advisories - Mandrake update for kdbase/kdelibs	web.archive.org text/html	SECUNIA 13477
Gentoo Linux Documentation -- kdelibs, kdbase: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200412-16
404 - Page not found! - SEC Consult	web.archive.org text/html Inactive Link Not Archived	★ MISC www.sec-consult.com/index.php?id=118
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 12248
	www.kde.org text/plain	CONFIRM www.kde.org/info/security/advisory-20041209-1.txt
Advisories - Mandriva	www.mandriva.com text/html	MANDRAKE MDKSA-2004:150
KDE Plaintext Password Disclosure Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	BID 11866
Secunia - Advisories - Gentoo update for kdelibs / kdbase	web.archive.org text/html	SECUNIA 13560
'Password Disclosure for SMB Shares in KDE's Konqueror' - MARC	marc.info text/html	BUGTRAQ 20041129 Password Disclosure for SMB Shares in KDE's Konqueror
No Description Provided	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20041129 Password Disclosure for SMB Shares in KDE's Konqueror

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

System	Product	Version	Architecture	Operating System	Kernel	Language
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	3.2	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	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	x86_64	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
cpe:2.3:o:kde:kde:3.2:*:*:*:*:*:						

cpe:2.3:o:kde:kde:3.2.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.2.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.2.3:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.3:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.3.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.3.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.2.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.2.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.2.3:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.3:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.3.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.3.2:*:*:*:*:*:
cpe:2.3:o:mandrakesoft:mandrake_linux:10.0:*:*:*:*:*:
cpe:2.3:o:mandrakesoft:mandrake_linux:10.0*:amd64:*:*:*:*:
cpe:2.3:o:mandrakesoft:mandrake_linux:10.1:*:*:*:*:*:
cpe:2.3:o:mandrakesoft:mandrake_linux:10.1*:x86_64:*:*:*:*:
cpe:2.3:o:mandrakesoft:mandrake_linux:10.0:*:*:*:*:*:
cpe:2.3:o:mandrakesoft:mandrake_linux:10.0*:amd64:*:*:*:*:
cpe:2.3:o:mandrakesoft:mandrake_linux:10.1:*:*:*:*:*:
cpe:2.3:o:mandrakesoft:mandrake_linux:10.1*:x86_64:*:*:*:*:
cpe:2.3:o:redhat:fedora_core:core_2.0:*:*:*:*:*:
cpe:2.3:o:redhat:fedora_core:core_3.0:*:*:*:*:*:
cpe:2.3:o:redhat:fedora_core:core_2.0:*:*:*:*:*:
cpe:2.3:o:redhat:fedora_core:core_3.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)