



CVE-2003-0690

Published on: 09/18/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:45 PM UTC

CVE-2003-0690

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

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

KDM in KDE 3.1.3 and earlier does not verify whether the pam_setcred function call succeeds, which may allow attackers to gain root privileges by triggering error conditions within PAM modules, as demonstrated in certain configurations of the MIT pam_krb5 module.

CVE-2003-0690 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Debian -- Security Information -- DSA-388-1
kdebase

[www.debian.org](#)
Deprecated Link
[text/html](#)

[DEBIAN DSA-388](#)

redhat.com | Red Hat Support

[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2003:289](#)

Mandriva Security Advisories

[www.mandriva.com](#)
[text/html](#)

[MANDRAKE MDKSA-2003:091](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL oval:org.mitre.oval:def:193](#)

Debian -- Security Information -- DSA-443-1
xfree86

[www.debian.org](#)
Deprecated Link
[text/html](#)

[DEBIAN DSA-443](#)

[suse-security] pam_krb5 & kdm: local root compromise (or misconfiguration?)	web.archive.org text/html Inactive Link Not Archived	 MISC cert.uni-stuttgart.de/archive/suse/security/2002/12/msg00101.html
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:286
redhat.com Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2003:270
Support	www.redhat.com text/html	 REDHAT RHSA-2003:287
	Patch Vendor Advisory www.kde.org text/plain	 CONFIRM www.kde.org/info/security/advisory-20030916-1.txt
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:288
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLA-2003:747
'[KDE SECURITY ADVISORY] KDM vulnerabilities' - MARC	marc.info text/html	 BUGTRAQ 20030916 [KDE SECURITY ADVISORY] KDM vulnerabilities

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	1.1	All	All	All
Operating System	Kde	Kde	1.1.1	All	All	All
Operating System	Kde	Kde	1.1.2	All	All	All
Operating System	Kde	Kde	1.2	All	All	All
Operating System	Kde	Kde	2.0	All	All	All
Operating System	Kde	Kde	2.0.1	All	All	All
Operating System	Kde	Kde	2.0_beta	All	All	All
Operating System	Kde	Kde	2.1	All	All	All

Operating System	Kde	Kde	2.1.1	All	All	All
Operating System	Kde	Kde	2.1.2	All	All	All
Operating System	Kde	Kde	2.2	All	All	All
Operating System	Kde	Kde	2.2.1	All	All	All
Operating System	Kde	Kde	2.2.2	All	All	All
Operating System	Kde	Kde	3.0	All	All	All
Operating System	Kde	Kde	3.0.1	All	All	All
Operating System	Kde	Kde	3.0.2	All	All	All
Operating System	Kde	Kde	3.0.3	All	All	All
Operating System	Kde	Kde	3.0.3a	All	All	All
Operating System	Kde	Kde	3.0.4	All	All	All
Operating System	Kde	Kde	3.0.5	All	All	All
Operating System	Kde	Kde	3.0.5a	All	All	All
Operating System	Kde	Kde	3.0.5b	All	All	All
Operating System	Kde	Kde	3.1	All	All	All
Operating System	Kde	Kde	3.1.1	All	All	All
Operating System	Kde	Kde	3.1.1a	All	All	All
Operating System	Kde	Kde	3.1.2	All	All	All
Operating System	Kde	Kde	3.1.3	All	All	All
Operating System	Kde	Kde	1.1	All	All	All
Operating System	Kde	Kde	1.1.1	All	All	All
Operating System	Kde	Kde	1.1.2	All	All	All
Operating System	Kde	Kde	1.2	All	All	All

Operating System	Kde	Kde	2.0	All	All	All
Operating System	Kde	Kde	2.0.1	All	All	All
Operating System	Kde	Kde	2.0_beta	All	All	All
Operating System	Kde	Kde	2.1	All	All	All
Operating System	Kde	Kde	2.1.1	All	All	All
Operating System	Kde	Kde	2.1.2	All	All	All
Operating System	Kde	Kde	2.2	All	All	All
Operating System	Kde	Kde	2.2.1	All	All	All
Operating System	Kde	Kde	2.2.2	All	All	All
Operating System	Kde	Kde	3.0	All	All	All
Operating System	Kde	Kde	3.0.1	All	All	All
Operating System	Kde	Kde	3.0.2	All	All	All
Operating System	Kde	Kde	3.0.3	All	All	All
Operating System	Kde	Kde	3.0.3a	All	All	All
Operating System	Kde	Kde	3.0.4	All	All	All
Operating System	Kde	Kde	3.0.5	All	All	All
Operating System	Kde	Kde	3.0.5a	All	All	All
Operating System	Kde	Kde	3.0.5b	All	All	All
Operating System	Kde	Kde	3.1	All	All	All
Operating System	Kde	Kde	3.1.1	All	All	All
Operating System	Kde	Kde	3.1.1a	All	All	All
Operating System	Kde	Kde	3.1.2	All	All	All
Operating System	Kde	Kde	3.1.3	All	All	All

cpe:2.3:o:kde:kde:1.1:*****:
cpe:2.3:o:kde:kde:1.1.1:*****:
cpe:2.3:o:kde:kde:1.1.2:*****:
cpe:2.3:o:kde:kde:1.2:*****:
cpe:2.3:o:kde:kde:2.0:*****:
cpe:2.3:o:kde:kde:2.0.1:*****:
cpe:2.3:o:kde:kde:2.0_beta:*****:
cpe:2.3:o:kde:kde:2.1:*****:
cpe:2.3:o:kde:kde:2.1.1:*****:
cpe:2.3:o:kde:kde:2.1.2:*****:
cpe:2.3:o:kde:kde:2.2:*****:
cpe:2.3:o:kde:kde:2.2.1:*****:
cpe:2.3:o:kde:kde:2.2.2:*****:
cpe:2.3:o:kde:kde:3.0:*****:
cpe:2.3:o:kde:kde:3.0.1:*****:
cpe:2.3:o:kde:kde:3.0.2:*****:
cpe:2.3:o:kde:kde:3.0.3:*****:
cpe:2.3:o:kde:kde:3.0.3a:*****:
cpe:2.3:o:kde:kde:3.0.4:*****:
cpe:2.3:o:kde:kde:3.0.5:*****:
cpe:2.3:o:kde:kde:3.0.5a:*****:
cpe:2.3:o:kde:kde:3.0.5b:*****:
cpe:2.3:o:kde:kde:3.1:*****:
cpe:2.3:o:kde:kde:3.1.1:*****:
cpe:2.3:o:kde:kde:3.1.1a:*****:
cpe:2.3:o:kde:kde:3.1.2:*****:
cpe:2.3:o:kde:kde:3.1.3:*****:
cpe:2.3:o:kde:kde:1.1:*****:
cpe:2.3:o:kde:kde:1.1.1:*****:

cpe:2.3:o:kde:kde:1.1.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:1.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.0:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.0.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.0_beta:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.1.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.1.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.2.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:2.2.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0.3:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0.3a:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0.4:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0.5:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0.5a:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.0.5b:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.1.1:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.1.1a:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.1.2:*:*:*:*:*:
cpe:2.3:o:kde:kde:3.1.3:*:*:*:*:*:

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](#)