



# CVE-2007-3820

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

## Summary

<b>CVE</b>	CVE-2007-3820
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-07-17 01:30:00 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	konqueror/konq_combo.cc in Konqueror 3.5.7 allows remote attackers to spoof the data: URI scheme in the address bar via

## Risk And Classification

**Primary CVSS:** v2.0 2.6 from nvd@nist.gov

AV:N/AC:H/Au:N/C:N/I:P/A:N

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:H/Au:N/C:N/I:P/A:N

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kde	Konqueror	3.5.7	All	All	All

## Vendor Declared Affected Products

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

## References

Reference	Source
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da266
Support	af854a3a-2127-422b-91ae-364da266
Fedora update for kdelibs - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266
SecurityFocus	af854a3a-2127-422b-91ae-364da266
SecurityFocus	af854a3a-2127-422b-91ae-364da266
Fedora update for kbase - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266
Ubuntu update for kbase and kdelibs - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266
SecurityReason - Opera/Konqueror: data: URL scheme address bar spoofing	af854a3a-2127-422b-91ae-364da266
KDE Konqueror Address Bar URI Spoofing Vulnerability	af854a3a-2127-422b-91ae-364da266
RETIRED: Konqueror Web Browser Data: URL Scheme Address Bar Spoofing Vulnerability	af854a3a-2127-422b-91ae-364da266
Webmail - OVH	af854a3a-2127-422b-91ae-364da266
Red Hat update for kdelibs - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266
KDE Konqueror 'data:' URL Display Bug Lets Remote Users Spoof the Address Bar - SecurityTracker	af854a3a-2127-422b-91ae-364da266
Support	af854a3a-2127-422b-91ae-364da266
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da266
Advisories - Mandriva Linux	af854a3a-2127-422b-91ae-364da266
[SECURITY] Fedora Core 6 Update: kdelibs-3.5.7-1.fc6	af854a3a-2127-422b-91ae-364da266
www.kde.org/info/security/advisory-20070816-1.txt	af854a3a-2127-422b-91ae-364da266
Mandriva update for konqueror - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266
Fedora update for kbase - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266
osvdb.org/37242	af854a3a-2127-422b-91ae-364da266
[SECURITY] Fedora 7 Update: kbase-3.5.7-13.1.fc7	af854a3a-2127-422b-91ae-364da266
Red Hat update for kbase - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266
USN-502-1: KDE vulnerabilities   Ubuntu	af854a3a-2127-422b-91ae-364da266
Google	af854a3a-2127-422b-91ae-364da266
Konqueror "data:" URI Scheme Address Bar Spoofing - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

## Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-09-05	Mark J Cox	This issue did not affect Red Hat Enterprise Linux 2.1 or 3. For Red Hat Enterprise Linux 4 and 5

## Legacy QID Mappings

[690274](#) Free Berkeley Software Distribution (FreeBSD) Security Update for konquerer (14ad2a28-66d2-11dc-b25f-02e0185f8d72)

© [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](#)