CVE-2006-0019

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-0019
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-20 21:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Heap-based buffer overflow in the encodeURI and decodeURI functions in the kjs JavaScript interpreter engine in KDE 3.2.

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

EPSS: 0.063870000 probability, percentile 0.910450000 (date 2026-04-16)

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

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	3.2.0	All	All	All
Operating System	Kde	Kde	3.2.0_beta1	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	3.2.x	All	All	All
Operating System	Kde	Kde	3.3	All	All	All
Operating System	Kde	Kde	3.3.0	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	3.3.x	All	All	All
Operating System	Kde	Kde	3.4	All	All	All
Operating System	Kde	Kde	3.4.0	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	3.5.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Ubuntu update for kdelibs4c2 - Advisories - Secunia	af854a3a-2127-422b-91ae-364
Repository / Oval Repository	af854a3a-2127-422b-91ae-364
Gentoo Linux Documentation -- KDE kjs: URI heap overflow vulnerability	af854a3a-2127-422b-91ae-364
Secunia - Advisories - Fedora update for kdelibs	af854a3a-2127-422b-91ae-364
www.kde.org/info/security/advisory-20060119-1.txt	af854a3a-2127-422b-91ae-364
Secunia - Advisories - Red Hat update for kdelibs	af854a3a-2127-422b-91ae-364
Advisories - Mandriva Linux	af854a3a-2127-422b-91ae-364
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364
Secunia - Advisories - Slackware update for kdelibs	af854a3a-2127-422b-91ae-364
SUSE update for kdelibs3 - Advisories - Secunia	af854a3a-2127-422b-91ae-364
KDE kjs UTF-8 Encoded URI Buffer Overflow Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91ae-364
The Slackware Linux Project: Slackware Security Advisories	af854a3a-2127-422b-91ae-364

Support	af854a3a-2127-422b-91ae-364
ftp.kde.org/pub/kde/security_patches/post-3.4.3-kdelibs-kjs.diff	af854a3a-2127-422b-91ae-364
SecurityTracker.com Archives - KDE kjs Engine Buffer Overflow Lets Remote Users Execute Arbitrary Code	af854a3a-2127-422b-91ae-364
Debian update for kdelibs - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364
SecurityFocus	af854a3a-2127-422b-91ae-364
Debian -- Security Information -- DSA-948-1 kdelibs	af854a3a-2127-422b-91ae-364
kjs encodeuri/decodeuri heap overflow - CXSecurity.com	af854a3a-2127-422b-91ae-364
KDE KJS Encodeuri / Decodeuri Remote Heap Overflow Vulnerability	af854a3a-2127-422b-91ae-364
SecurityFocus	af854a3a-2127-422b-91ae-364
SecurityFocus	af854a3a-2127-422b-91ae-364
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364
usn/usn-245-1 - Ubuntu: Linux for human beings	af854a3a-2127-422b-91ae-364
www.osvdb.org/22659	af854a3a-2127-422b-91ae-364
Gentoo update for kdelibs - Advisories - Secunia	af854a3a-2127-422b-91ae-364
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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 registred 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