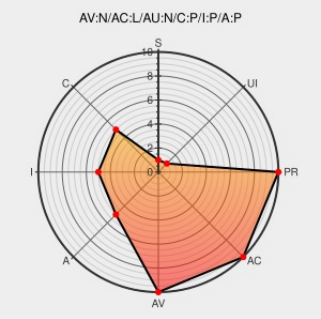
CVE-2004-0411

Published on: 05/20/2004 12:00:00 AM UTC

Last Modified on: 02/28/2022 05:16:00 PM UTC

CVE-2004-0411

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Konqueror from Kde contain the following vulnerability:

The URI handlers in Konqueror for KDE 3.2.2 and earlier do not properly filter "-" characters that begin a hostname in a (1) telnet, (2) rlogin, (3) ssh, or (4) mailto URI, which allows remote attackers to manipulate the options that are passed to the associated programs, possibly to read arbitrary files or execute arbitrary code.

CVE-2004-0411 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Secunia - Advisories - Multiple Browsers Telnet URI Handler File Manipulation Vulnerability	web.archive.org text/html	SECUNIA 11602
Malformed Request	www.securityfocus.com text/html Inactive Link Not Archived	FEDORA FEDORA-2004-122
O-146: kdelibs Package Vulnerabilities	web.archive.org text/html Inactive Link Not Archived	CIAC O-146
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2004:222
Debian -- Security Information -- DSA-518-1 kdelibs	www.debian.org	DEBIAN DSA-518

	Depreciated Link text/html	
'KDE Security Advisory: URI Handler Vulnerabilities' - MARC	marc.info text/html	BUGTRAQ 20040517 KDE Security Advisory: URI Handler Vulnerabilities
	Patch Vendor Advisory www.kde.org text/plain	CONFIRM www.kde.org/info/security/advisory-20040517-1.txt
Malformed Request	www.securityfocus.com text/html Inactive Link Not Archived	FEDORA FEDORA-2004-121
SecurityFocus	Vendor Advisory www.securityfocus.com text/html	BUGTRAQ 20040513 Opera Telnet URI Handler Vulnerability also applies to other browsers
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SuSE-SA:2003:014
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF kde-url-handler-gain-access(16163)
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 6107
KDE Multiple URI Handler Vulnerabilities	cve.report (archive) text/html	BID 10358
Home - Conectiva	distro.conectiva.com.br text/html	CONECTIVA CLA-2004:843
Gentoo Linux Documentation -- KDE URI Handler Vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-200405-11
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:954
The Slackware Linux Project: Slackware Security Advisories	www.slackware.org text/html	SLACKWARE SSA:2004-238

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kde	Konqueror	All	All	All	All
Application	Opera Software	Opera Web Browser	9.10	All	All	All
Application	Opera Software	Opera Web Browser	9.10	All	All	All

cpe:2.3:a:kde:konqueror:*:*:*:*:*:*:*:*:

cpe:2.3:a:opera_software:opera_web_browser:9.10:*:*:*:*:*:*:*:

cpe:2.3:a:opera_software:opera_web_browser:9.10:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→