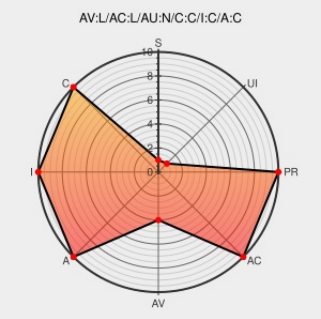
CVE-2002-1247

Published on: 11/14/2002 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1247

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



Certain versions of Kde from Kde contain the following vulnerability:

Buffer overflow in LISa allows local users to gain access to a raw socket via a long LOGNAME environment variable for the resLISa daemon.

CVE-2002-1247 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
N-020: Red Hat Multiple Vulnerabilities in KDE	web.archive.org, text/html, Inactive Link, Not Archived	CIAC N-020
redhat.com | Red Hat Support	www.redhat.com, text/html	REDHAT RHSA-2002:220
ISS X-Force Database: kde-kdenetwork-reslisa-bo (10592): KDE kdenetwork resLISa module LOGNAME buffer overflow	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	XF kde-kdenetwork-reslisa-bo(10592)
'GLSA: kdelibs' - MARC	marc.info, text/html	BUGTRAQ 20021114 GLSA: kdelibs
Advisories - Mandriva Linux	www.mandriva.com, text/html	MANDRAKE MDKSA-2002:080

No Description Provided	web.archive.org text/html Inactive Link Not Archived	VULNWATCH 20021111 iDEFENSE Security Advisory 11.11.02: Buffer Overflow in KDE resLISa
No Description Provided	marc.info text/html	BUGTRAQ 20021111 iDEFENSE Security Advisory 11.11.02: Buffer Overflow in KDE resLISa
'KDE Security Advisory: resLISa / LISa Vulnerabilities' - MARC	marc.info text/html	BUGTRAQ 20021112 KDE Security Advisory: resLISa / LISa Vulnerabilities
KDE Network RESLISA LOGNAME Local Buffer Overflow Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	BID 6157
Accenture | Let there be change	www.idefense.com text/plain	MISC www.idefense.com/advisory/11.11.02.txt
Debian -- Security Information -- DSA-193-1 kdenetwork	Patch Vendor Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-193

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	2.0	All	All	All
Operating System	Kde	Kde	2.1	All	All	All
Operating System	Kde	Kde	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	2.0	All	All	All
Operating System	Kde	Kde	2.1	All	All	All
Operating System	Kde	Kde	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
Application	Kde	Klisa	2.2.2	All	All	All
Application	Kde	Klisa	2.2.2	All	All	All
Application	Lisa	Lisa	0.1	All	All	All
Application	Lisa	Lisa	0.1.2	All	All	All
Application	Lisa	Lisa	0.1	All	All	All
Application	Lisa	Lisa	0.1.2	All	All	All

cpe:2.3:o:kde:kde:2.0:*:*:*:*:*:*:*:

cpe:2.3:o:kde:kde:2.1:*:*:*:*:*:*:*:

cpe:2.3:o:kde:kde: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:2.0:*:*:*:*:*:*:*:

cpe:2.3:o:kde:kde:2.1:*:*:*:*:*:*:*:

cpe:2.3:o:kde:kde: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:a:kde:klisa:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:kde:klisa:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:lisa:lisa:0.1:*:*:*:*:*:*:*:

cpe:2.3:a:lisa:lisa:0.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:lisa:lisa:0.1:*:*:*:*:*:*:*:

cpe:2.3:a:lisa:lisa:0.1.2:*:*:*:*:*:*:*:

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 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.

CVE.report and Source URL Uptime Status status.cve.report