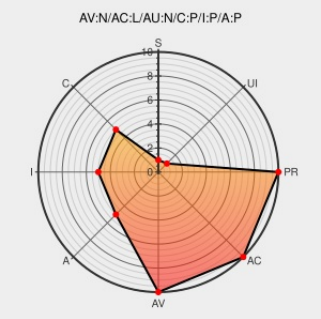
# CVE-2002-1281

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

Last Modified on: 03/23/2021 11:26:02 PM UTC

## CVE-2002-1281

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




Certain versions of Kde from Kde contain the following vulnerability:

Unknown vulnerability in the rlogin KIO subsystem (rlogin.protocol) of KDE 2.x 2.1 and later, and KDE 3.x 3.0.4 and earlier, allows local and remote attackers to execute arbitrary code via a certain URL.

CVE-2002-1281 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 |
|---|---|---|
| No Description Provided | www.linux-mandrake.com<br>Inactive Link Not Archived | MANDRAKE MDKSA-2002:079 |
| redhat.com \| Red Hat Support | Patch<br>Vendor Advisory<br>www.redhat.com<br>text/html | REDHAT RHSA-2002:220 |
| 'KDE Security Advisory: rlogin.protocol and telnet.protocol URL KIO Vulnerability' - MARC | marc.info<br>text/html | BUGTRAQ 20021112 KDE Security Advisory: rlogin.protocol and telnet.protocol URL KIO Vulnerability |
| | Patch<br>Vendor Advisory<br>www.kde.org<br>text/plain | CONFIRM www.kde.org/info/security/advisory-20021111-1.txt |

| | | |
|---|---|---|
| 'GLSA: kdelibs' - MARC | marc.info<br>text/html | BUGTRAQ 20021114 GLSA: kdelibs |
| Debian -- Security Information -- DSA-204-1 kdelibs | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-204 |
| No Description Provided | ftp.caldera.com<br>Inactive Link Not Archived | CALDERA CSSA-2003-012.0 |
| KDE KIO Subsystem Network Protocol Implementation Arbitrary Command Execution Vulnerability | Patch<br>Vendor Advisory<br>cve.report (archive)<br>text/html | BID 6182 |
| Secunia - Advisories - OpenLinux update to kdelibs | web.archive.org<br>text/html | SECUNIA 8298 |
| ISS X-Force Database: kde-rlogin-command-execution (10602): KDE kdelib KIO rlogin:// URL handler remote shell command execution | Vendor Advisory<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | XF kde-rlogin-command-execution(10602) |



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 | 2.1 | 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 | Kde | Kde | 3.0.3 | All | All | All |

System

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Kde | Kde | 3.0.4 | 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 | 3.0.4 | All | All | All |

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:3.0.4:*:*:*:*:*:*:*:

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:3.0.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→