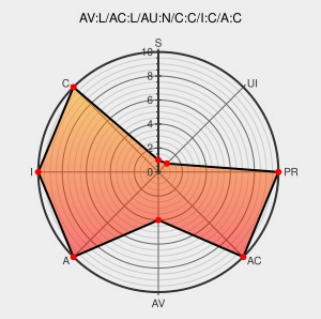
CVE-1999-1182

Published on: 07/17/1997 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:32 PM UTC

CVE-1999-1182

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



Certain versions of Openlinux Lite from Caldera contain the following vulnerability:

Buffer overflow in run-time linkers (1) ld.so or (2) ld-linux.so for Linux systems allows local users to gain privileges by calling a setuid program with a long program name (argv[0]) and forcing ld.so/ld-linux.so to report an error.

CVE-1999-1182 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
'ld.so vulnerability' - MARC	marc.info text/html	BUGTRAQ 19970722 ld.so vulnerability
'KSR[T] Advisory #2: ld.so' - MARC	marc.info text/html	BUGTRAQ 19970717 KSR[T] Advisory #2: ld.so
'An old ld-linux.so hole' - MARC	marc.info text/html	BUGTRAQ 19980204 An old ld-linux.so hole

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Caldera	Openlinux Lite	1.1	All	All	All
Operating System	Caldera	Openlinux Lite	1.1	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Application	Delix	Dld	5.2	All	All	All
Application	Delix	Dld	5.2	All	All	All
Operating System	Lst	Lst Power Linux	2.2	All	All	All
Operating System	Lst	Lst Power Linux	2.2	All	All	All
Operating System	Redhat	Linux	4.0	All	All	All
Operating System	Redhat	Linux	4.1	All	All	All
Operating System	Redhat	Linux	4.2	All	All	All
Operating System	Redhat	Linux	4.0	All	All	All
Operating System	Redhat	Linux	4.1	All	All	All
Operating System	Redhat	Linux	4.2	All	All	All
Operating System	Suse	Suse Linux	5.0	All	All	All
Operating System	Suse	Suse Linux	5.0	All	All	All

cpe:2.3:o:caldera:openlinux_lite:1.1:*:*:*:*:*:*:*:

cpe:2.3:o:caldera:openlinux_lite:1.1:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:delix:dld:5.2:*:*:*:*:*:*:*:

cpe:2.3:a:delix:dld:5.2:*:*:*:*:*:*:*:

cpe:2.3:o:lst:lst_power_linux:2.2:*:*:*:*:*:*:*:

cpe:2.3:o:lst:lst_power_linux:2.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:4.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:4.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:4.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:linux:4.2:*:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux:5.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→