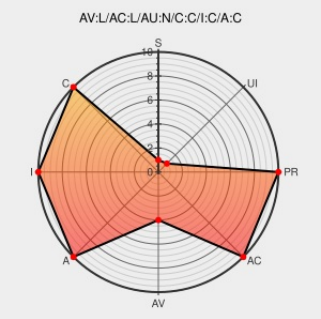
CVE-2003-0961

Published on: 12/02/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:46 PM UTC

CVE-2003-0961

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



Certain versions of Linux Kernel from Linux contain the following vulnerability:

Integer overflow in the do_brk function for the brk system call in Linux kernel 2.4.22 and earlier allows local users to gain root privileges.

CVE-2003-0961 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
Debian -- Security Information -- DSA-423-1 linux-kernel-2.4.17-ia64	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-423
Debian -- Security Information -- DSA-450-1 linux-kernel-2.4.19-mips	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-450
Secunia - Advisories - Debian update for Kernel	web.archive.org, text/html	SECUNIA 10333
'[iSEC] Linux kernel do_brk() vulnerability details' - MARC	marc.info, text/html	BUGTRAQ 20031204 [iSEC] Linux kernel do_brk() vulnerability details
CERT/CC Vulnerability Note VU#301156	US Government Resource, www.kb.cert.org, text/html	CERT-VN VU#301156

NOVELL: Broken Link - 404 Error Pages	web.archive.org text/html Inactive Link Not Archived	SUSE SuSE-SA:2003:049
Debian -- Security Information -- DSA-439-1 linux-kernel-2.4.16-arm	www.debian.org Depreciated Link text/html	DEBIAN DSA-439
Debian -- Security Information -- DSA-403-1 kernel-image-2.4.18-1-alpha, kernel-image-2.4.18-1-i386, kernel-source-2.4.18	Patch Vendor Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-403
Debian -- Security Information -- DSA-475-1 linux-kernel-2.4.18-hppa	www.debian.org Depreciated Link text/html	DEBIAN DSA-475
Debian -- Security Information -- DSA-417-1 linux-kernel-2.4.18-powerpc+alpha	www.debian.org Depreciated Link text/html	DEBIAN DSA-417
Debian -- Security Information -- DSA-470-1 linux-kernel-2.4.17-hppa	www.debian.org Depreciated Link text/html	DEBIAN DSA-470
Secunia - Advisories - Astaro update for Kernel	web.archive.org text/html	SECUNIA 10338
Home - Conectiva	distro.conectiva.com.br text/html	CONECTIVA CLA-2003:796
'Hot fix for do_brk bug' - MARC	marc.info text/x-c	BUGTRAQ 20031204 Hot fix for do_brk bug
Mandriva Security Advisories	www.mandriva.com text/html	MANDRAKE MDKSA-2003:110
Secunia - Advisories - Red Hat update for Kernel	web.archive.org text/html	SECUNIA 10329
Secunia - Advisories - Mandrake update for Kernel	web.archive.org text/html	SECUNIA 10330
Debian -- Security Information -- DSA-440-1 linux-kernel-2.4.17-powerpc-apus	www.debian.org Depreciated Link text/html	DEBIAN DSA-440
Secunia - Advisories - Linux Kernel "do_brk()" Privilege Escalation Vulnerability	web.archive.org text/html	SECUNIA 10328
'SmoothWall Project Security Advisory SWP-2004:001' - MARC	marc.info text/html	BUGTRAQ 20040112 SmoothWall Project Security Advisory SWP-2004:001
Debian -- Security Information -- DSA-433-1 kernel-patch-2.4.17-mips	www.debian.org Depreciated Link text/html	DEBIAN DSA-433
Securityin a digital world	isec.pl application/pdf	MISC isec.pl/papers/linux_kernel_do_brk.pdf
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:368
Debian -- Security Information -- DSA-442-1 linux-kernel-2.4.17-s390	www.debian.org Depreciated Link	DEBIAN DSA-442

	text/html	
redhat.com | Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2003:389

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	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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