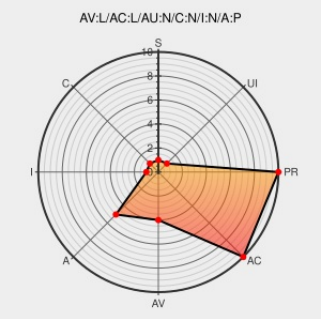
CVE-2005-2456

Published on: 08/04/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2456

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



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

Array index overflow in the xfrm_sk_policy_insert function in xfrm_user.c in Linux kernel 2.6 allows local users to cause a denial of service (oops or deadlock) and possibly execute arbitrary code via a p->dir value that is larger than XFRM_POLICY_OUT, which is used as an index in the sock->sk_policy array.

CVE-2005-2456 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:663
Linux Kernel XFRM Array Index Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 14477
Security Announcement	web.archive.org text/html Inactive Link Not Archived	ot SUSE SUSE-SA:2005:050
[PATCH] possible overflow of sock->sk_policy	Patch www.mail-archive.com text/x-diff	MISC www.mail-archive.com/netdev@vger.kernel.org/msg00520.html

Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-1878
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRAKE MDKSA-2005:219
SecurityFocus	www.securityfocus.com text/html	FEDORA FLSA:157459-3
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch www.kernel.org text/html Inactive Link Not Archived	CONFIRM www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=blobdiff;h=8da3e25b2c4c1f305fd85428d3a9eb62b543bfba;hp=ecade489
Debian -- Security Information -- DSA-922-1 kernel-source-2.6.8	www.debian.org Depreciated Link text/html	DEBIAN DSA-922
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:514
Debian -- Security Information -- DSA-921-1 kernel-source-2.4.27	www.debian.org Depreciated Link text/html	DEBIAN DSA-921
Secunia - Advisories - Red Hat update for kernel	web.archive.org text/html	SECUNIA 17002
Secunia - Advisories - Red Hat update for kernel	web.archive.org text/html	SECUNIA 17073
USN-169-1: Linux kernel vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-169-1
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRAKE MDKSA-2005:220
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10858
Secunia - Advisories - Ubuntu update for kernel	web.archive.org text/html	SECUNIA 16500
Secunia - Advisories - Debian update for kernel-source-2.4.27	web.archive.org text/html	SECUNIA 18059
Secunia - Advisories - Linux Kernel xfrm Array Indexing Overflow Vulnerability	web.archive.org text/html	SECUNIA 16298
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch www.kernel.org text/html	CONFIRM www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=comm
Secunia - Advisories - Mandriva update for kernel	web.archive.org text/html	SECUNIA 17826
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF linux-kernel-xfrm-dos(21710)
Secunia - Advisories - Debian update for kernel-source-2.6.8	web.archive.org text/html	SECUNIA 18056

source-2.6.8

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	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→