CVE-2010-3875

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-3875
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-03 20:00:00 UTC
Updated	2023-02-13 04:27:00 UTC
Description	The ax25_getname function in net/ax25/af_ax25.c in the Linux kernel before 2.6.37-rc2 does not initialize a certain structure

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.37	-	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc1	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.37	-	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc1	All	All

References

Reference	Source	Link
404: File not found	CONFIRM	www.kernel.org
oss-security - Re: CVE request: kernel stack infoleaks	MLIST	openwall.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
oss-security - CVE request: kernel stack infoleaks	MLIST	openwall.com
Linux Kernel Multiple 'net/' Subsystems Local Information Disclosure Vulnerabilities	BID	www.securityfoc
'[PATCH 1/3] net: ax25: fix information leak to userland' - MARC	MLIST	marc.info

mandriva.com	MANDRIVA	www.mandriva.c
Debian -- Security Information -- DSA-2126-1 linux-2.6	DEBIAN	www.debian.org
mandriva.com	MANDRIVA	www.mandriva.c
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
649713 – (CVE-2010-3875) CVE-2010-3875 kernel: net/ax25/af_ax25.c: reading uninitialized stack memory	CONFIRM	bugzilla.redhat.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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