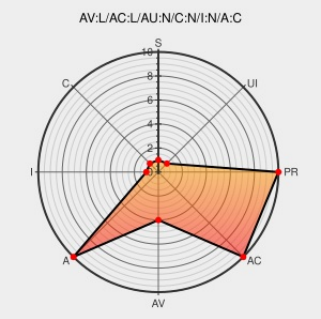
CVE-2010-2954

Published on: 09/03/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:21:00 AM UTC

CVE-2010-2954

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The irda_bind function in net/irda/af_irda.c in the Linux kernel before 2.6.36-rc3-next-20100901 does not properly handle failure of the irda_open_tsap function, which allows local users to cause a denial of service (NULL pointer dereference and panic) and possibly have unspecified other impact via multiple unsuccessful calls to bind on an AF_IRDA (aka PF_IRDA) socket.

CVE-2010-2954 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
[security-announce] SUSE Security Announcement: Realtime Linux Kernel (S	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SA:2011:007
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory, www.vupen.com, text/html	VUPEN ADV-2010-2430
No Description Provided	Broken Link, git.kernel.org, text/html, Inactive Link, Not Archived	MISC git.kernel.org/?p=linux/kernel/git/davem/net-2.6.git%3Ba=commit%3Bh=628e300cccaa628d8fb92aa28cb7530a3d5f2257

[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SA:2010:041
404: File not found	Broken Link www.kernel.org text/html Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/next/patch-v2.6.36-rc3-next-20100901.bz2
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SA:2010:052
Linux Kernel "irda_bind()" Object Cleanup Vulnerability - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 41234
Bug 628770 – CVE-2010-2954 kernel: NULL deref and panic in irda	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=628770
USN-1000-1: Linux kernel vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-1000-1
Tavis Ormandy na Twitterze: "Mail me if you want a testcase for CVE-2010-2954, although it's simple enough, just make bind() on an AF_IRDA socket fail a few times."	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/taviso/statuses/22635752128
[PATCH] irda: Correctly clean up self->ias_obj on irda_bind() failure. — Linux Network Development	Patch Third Party Advisory www.spinics.net text/x-diff	MLIST [netdev] 20100830 [PATCH] irda: Correctly clean up self->ias_obj on irda_bind() failure.
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SA:2010:050
SUSE update for kernel - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 41512
'[oss-security] CVE-2010-2954 kernel: irda null ptr deref' - MARC	Patch Third Party Advisory marc.info text/html	MLIST [oss-security] 20100901 CVE-2010-2954 kernel: irda null ptr deref
CVE-2010-2954 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2010-2954
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2010-2266
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2011-0298

IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF kernel-irdabind-dos(61522)

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	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.36	-	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc2	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Operating System	Linux	Linux Kernel	2.6.36	-	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.36	rc2	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	-	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	11	-	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

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

cpe:2.3:o:linux:linux_kernel:2.6.36:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc2:*:*:*:*:*:*:

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

cpe:2.3:o:linux:linux_kernel:2.6.36:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36:rc2:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:-:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→