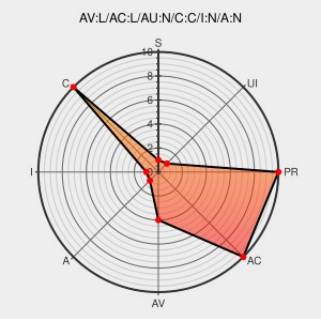
CVE-2013-3233

Published on: 04/22/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:30 PM UTC

CVE-2013-3233

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



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

The llcp_sock_recvmsg function in net/nfc/llcp/sock.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable and a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.

CVE-2013-3233 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
NFC: llcp: fix info leaks via msg_name in llcp_sock_recvmsg() · torvalds/linux@d26d650 · GitHub	Vendor Advisory, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/d26d6504f23e803824e8ebd14e52d4fc0a0b09cb
USN-1837-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com, text/html	UBUNTU USN-1837-1
oss-security - Linux kernel: more net info leak fixes for v3.9	www.openwall.com, text/html	MLIST [oss-security] 20130414 Linux kernel: more net info leak fixes for v3.9
LKML: Linus Torvalds: Linux 3.9-rc7	Vendor Advisory, lkml.org, text/xml	MLIST [linux-kernel] 20130414 Linux 3.9-rc7

[SECURITY] Fedora 17 Update: kernel-3.8.11-100.fc17	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-6999
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=d26d6504f23e803824e8ebd14e52d4fc0a0b09cb
Support / Security / Advisories / / MDVSA-2013:176 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:176
[SECURITY] Fedora 18 Update: kernel-3.8.8-203.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-6537
openSUSE-SU-2013:1971-1: moderate: kernel: security and bugfix update	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1971

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	3.9	rc1	All	All
Operating System	Linux	Linux Kernel	3.9	rc2	All	All
Operating System	Linux	Linux Kernel	3.9	rc3	All	All
Operating System	Linux	Linux Kernel	3.9	rc4	All	All
Operating System	Linux	Linux Kernel	3.9	rc5	All	All
Operating System	Linux	Linux Kernel	3.9	rc1	All	All
Operating System	Linux	Linux Kernel	3.9	rc2	All	All
Operating System	Linux	Linux Kernel	3.9	rc3	All	All
Operating System	Linux	Linux Kernel	3.9	rc4	All	All
Operating System	Linux	Linux Kernel	3.9	rc5	All	All
Operating System	Linux	Linux Kernel	All	rc6	All	All

cpe:2.3:o:linux:linux_kernel:3.9:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.9:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:rc6:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→