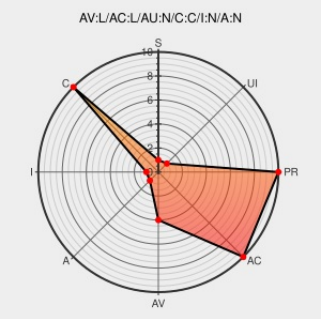
CVE-2013-3235

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

Last Modified on: 03/23/2021 11:28:29 PM UTC

CVE-2013-3235

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



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

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

CVE-2013-3235 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
tipc: fix info leaks via msg_name in recv_msg/recv_stream · torvalds/linux@60085c3 · GitHub	Vendor Advisory, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/60085c3d009b0df252547adb336d1ccca5ce52ec
[security-announce] openSUSE-SU-2013:1187-1: important: 3.0.80 kernel up	lists.opensuse.org, text/html	SUSE openSUSE-SU-2013:1187
[security-announce] SUSE-SU-2013:1182-1: important: kernel update for SL	lists.opensuse.org, text/html	SUSE SUSE-SU-2013:1182
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
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=60085c3d009b0df252547adb336d1ccca5ce52ec
Support / Security / Advisories / / MDVSA-2013:176 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:176
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→