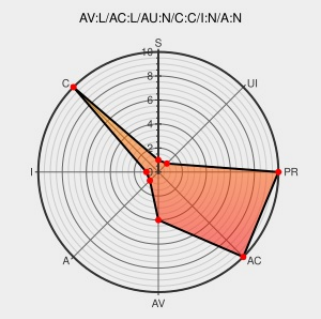
CVE-2013-3237

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

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

CVE-2013-3237

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



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

The vsock_stream_sendmsg function in net/vmw_vsock/af_vsock.c in the Linux kernel before 3.9-rc7 does not initialize 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-2013-3237 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
VSOCK: Fix missing msg_namelen update in vsock_stream_recvmsg() · torvalds/linux@d5e0d0f · GitHub	Vendor Advisory, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/d5e0d0f607a7a029c6563a0470d88255c89a8d11
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=d5e0d0f607a7a029c6563a0470d88255c89a8d11

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	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→