



CVE-2013-3223

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

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

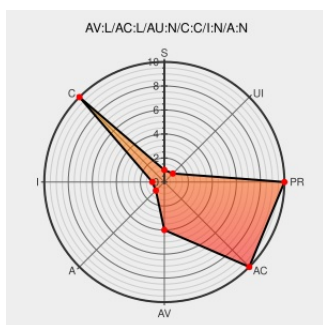
CVE-2013-3223

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

The ax25_rcvmsg function in net/ax25/af_ax25.c in the Linux kernel before 3.9-rc7 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted rcvmsg or rcvfrom system call.

CVE-2013-3223 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

COMPLETE

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

[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](#)

ax25: fix info leak via msg_name in ax25_rcvmsg() · torvalds/linux@ef3313e · GitHub

[github.com](#)
[text/html](#)

[CONFIRM](#)
[github.com/torvalds/linux/commit/ef3313e84acbf349caecae942ab3ab731471f1a1](#)

kernel/git/torvalds/linux.git - Linux kernel source tree

[Vendor Advisory](#)
[git.kernel.org](#)

[CONFIRM](#) [git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ef3313e84acbf349caecae942ab3ab731471f1a1](#)

[text/html](#)

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

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

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

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 →](#)