

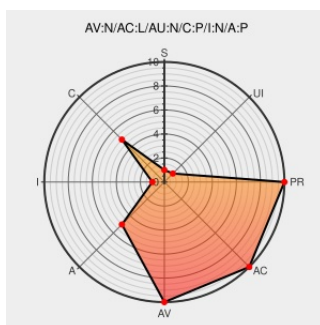


# CVE-2011-4914

Published on: 06/21/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:22:00 AM UTC

## CVE-2011-4914

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The ROSE protocol implementation in the Linux kernel before 2.6.39 does not verify that certain data-length values are consistent with the amount of data sent, which might allow remote attackers to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read) via crafted data to a ROSE socket.

CVE-2011-4914 has been assigned by [secalert@redhat.com](mailto:secalert@redhat.com) to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**NONE**

Confidentiality  
Impact

**PARTIAL**

Integrity  
Impact

**NONE**

Availability  
Impact

**PARTIAL**

## CVE References

Description

Tags

Link

[security-announce] SUSE-SU-2015:0812-1: important: Security update for

[Third Party Advisory](#)  
[lists.opensuse.org](#)  
[text/html](#)

[SUSE SUSE-SU-2015:0812](#)

oss-security - Re: CVE request: kernel: multiple issues in ROSE

[www.openwall.com](#)  
[text/html](#)

[MLIST \[oss-security\] 20111227 Re: CVE request: kernel: multiple issues in ROSE](#)

Bug 770777 – CVE-2011-1493 CVE-2011-4913 CVE-2011-4914 kernel: multiple issues in rose protocol

[Issue Tracking](#)  
[VDB Entry](#)  
[bugzilla.redhat.com](#)  
[text/html](#)

[CONFIRM bugzilla.redhat.com/show\\_bug.cgi?id=770777](#)

rose: Add length checks to CALL\_REQUEST parsing

[Exploit](#)  
[Patch](#)

[CONFIRM github.com/torvalds/linux/commit/e0bccd315db0c2f919e7fc9cb60db21d9986f52](#)

torvalds/linux@e0bccd3 · GitHub

github.com

text/html

No Description Provided

Patch

git.kernel.org

text/html

Inactive Link

Not Archived

MISC

git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=e0bccd315db0c2f919e7fcf9cb60db21d9986f52

404 Not Found

Broken Link

ftp.osuosl.org

text/plain

Inactive Link

Not Archived

CONFIRM

ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39

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](mailto: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 | 2.6.38   | All    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38   | rc1    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38   | rc2    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38   | rc3    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38   | rc4    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38   | rc5    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38   | rc6    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38   | rc7    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38   | rc8    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38.1 | All    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38.2 | All    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38.3 | All    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38.4 | All    | All     | All      |
| Operating System                         | Linux  | Linux Kernel | 2.6.38.5 | All    | All     | All      |

|                                                |        |                              |          |     |     |     |
|------------------------------------------------|--------|------------------------------|----------|-----|-----|-----|
| System                                         |        |                              |          |     |     |     |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.6 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.7 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | rc1 | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | rc2 | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | rc3 | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | rc4 | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | rc5 | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | rc6 | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | rc7 | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38   | rc8 | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.1 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.2 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.3 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.4 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.5 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.6 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | 2.6.38.7 | All | All | All |
| Operating System                               | Linux  | Linux Kernel                 | All      | All | All | All |
| Operating System                               | Novell | Suse Linux Enterprise Server | 10.0     | sp4 | All | All |
| Operating System                               | Novell | Suse Linux Enterprise Server | 10.0     | sp4 | All | All |
| cpe:2.3:o:linux:linux_kernel:2.6.38:*****:     |        |                              |          |     |     |     |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc1:*****: |        |                              |          |     |     |     |

|                                                    |
|----------------------------------------------------|
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc2:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc3:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc4:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc5:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc6:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc7:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc8:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38.1:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.2:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.3:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.4:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.5:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.6:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.7:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38:*:*:*:*:*:     |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc1:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc2:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc3:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc4:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc5:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc6:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc7:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38:rc8:*:*:*:*:*: |
| cpe:2.3:o:linux:linux_kernel:2.6.38.1:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.2:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.3:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.4:*:*:*:*:*:   |
| cpe:2.3:o:linux:linux_kernel:2.6.38.5:*:*:*:*:*:   |

|                                                                      |
|----------------------------------------------------------------------|
| cpe:2.3:o:linux:linux_kernel:2.6.38.6:****:*:                        |
| cpe:2.3:o:linux:linux_kernel:2.6.38.7:****:*:                        |
| cpe:2.3:o:linux:linux_kernel:****:*:                                 |
| cpe:2.3:o:novell:suse_linux_enterprise_server:10.0:sp4:*:*:ltss:*:*: |
| cpe:2.3:o:novell:suse_linux_enterprise_server:10.0:sp4:*:*:ltss:*:*: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)