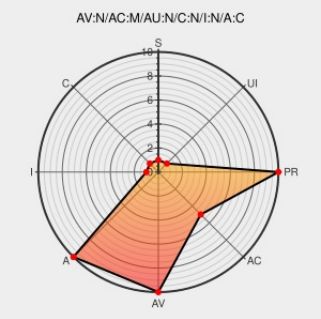
# CVE-2011-4348

Published on: 06/08/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:32:00 AM UTC

## CVE-2011-4348

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




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

Race condition in the sctp_rcv function in net/sctp/input.c in the Linux kernel before 2.6.29 allows remote attackers to cause a denial of service (system hang) via SCTP packets. NOTE: in some environments, this issue exists because of an incomplete fix for CVE-2011-2482.

CVE-2011-4348 has been assigned by secalert@redhat.com to track the vulnerability

### CVSS2 Score: 7.1 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| 404 Not Found | ftp.osuosl.org, text/plain, Inactive Link, Not Archived | CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.29 |
| 757143 – (CVE-2011-4348) CVE-2011-4348 kernel: incomplete fix for CVE-2011-2482 | Vendor Advisory, bugzilla.redhat.com, text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=757143 |
| oss-security - CVE-2011-4348 kernel: incomplete fix for CVE-2011-2482 | www.openwall.com, text/html | MLIST [oss-security] 20120305 CVE-2011-4348 kernel: incomplete fix for CVE-2011-2482 |
| kernel/git/torvalds/linux.git - Linux kernel source tree | web.archive.org, text/html | MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=ae53b5bd77719fed58086c5be60ce4f22bffe1c6 |

| | | |
|---|---|---|
| | Inactive Link Not Archived | |
| access.redhat.com \| CVE-2011-4348 | access.redhat.com text/html | MISC access.redhat.com/security/cve/CVE-2011-4348 |
| sctp: Fix another socket race during accept/peeloff · torvalds/linux@ae53b5b · GitHub | github.com text/html | CONFIRM github.com/torvalds/linux/commit/ae53b5bd77719fed58086c5be60ce4f22bffe1c6 |
| Red Hat Customer Portal | access.redhat.com text/html | MISC access.redhat.com/errata/RHSA-2012:0007 |



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 | 2.6.28 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.1 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.2 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.3 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.4 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.5 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.6 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.7 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.8 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.9 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.1 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.2 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.3 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Linux | Linux Kernel | 2.6.28.4 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.5 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.6 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.7 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.8 | All | All | All |
| Operating System | Linux | Linux Kernel | 2.6.28.9 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |

cpe:2.3:o:linux:linux_kernel:2.6.28:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.7:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.8:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.9:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.6:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.7:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.8:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.28.9:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→