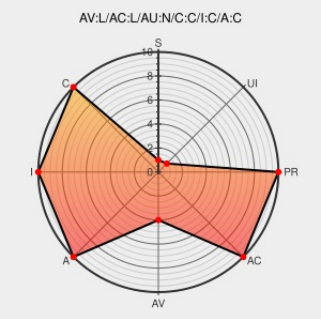
# CVE-2011-2517

Published on: 05/24/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:20:00 AM UTC

## CVE-2011-2517

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




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

Multiple buffer overflows in net/wireless/nl80211.c in the Linux kernel before 2.6.39.2 allow local users to gain privileges by leveraging the CAP_NET_ADMIN capability during scan operations with a long SSID value.

CVE-2011-2517 has been assigned by secalert@redhat.com to track the vulnerability

## CVSS2 Score: 7.2 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| kernel/git/torvalds/linux.git - Linux kernel source tree | Patch, Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived | MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=208c72f4fe44fe09577e7975ba0e7fa0278f3d03 |
| 718152 – (CVE-2011-2517) CVE-2011-2517 kernel: nl80211: missing check for valid SSID size in scan operations | Issue Tracking, Third Party Advisory, bugzilla.redhat.com, text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=718152 |
| access.redhat.com | Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived | REDHAT RHSA-2011:1212 |

| | | |
|---|---|---|
| oss-security - Re: CVE request: kernel: nl80211: missing check for valid SSID size in scan operations | Mailing List<br>Third Party Advisory<br>www.openwall.com<br>text/html | MLIST [oss-security] 20110701 Re: CVE request: kernel: nl80211: missing check for valid SSID size in scan operations |
| nl80211: fix check for valid SSID size in scan operations · torvalds/linux@208c72f · GitHub | Patch<br>Third Party Advisory<br>github.com<br>text/html | CONFIRM github.com/torvalds/linux/commit/208c72f4fe44fe09577e7975ba0e7fa0278f3d03 |
| 404 Not Found | Broken Link<br>ftp.osuosl.org<br>text/plain<br>Inactive Link Not Archived | CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39.2 |



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 | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 5.0 | All | All | All |

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

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

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→