

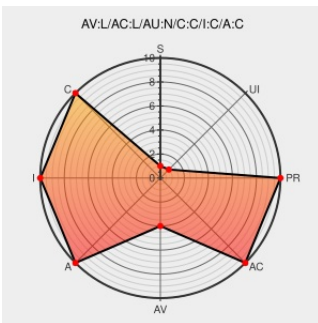


CVE-2011-2517

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

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

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

Third Party Advisory

www.openwall.com

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

Third Party Advisory

github.com

text/html

CONFIRM

github.com/torvalds/linux/commit/208c72f4fe44fe09577e7975ba0e7fa0278f3d03

404 Not Found

Broken Link

ftp.osuosl.org

text/plain

Inactive Link

Not Archived

CONFIRM

ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39.2

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	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 →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)