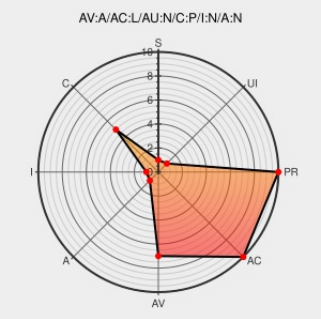
CVE-2010-4648

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

Last Modified on: 02/13/2023 03:20:00 AM UTC

CVE-2010-4648

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



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

The orinoco_ioctl_set_auth function in drivers/net/wireless/orinoco/wext.c in the Linux kernel before 2.6.37 does not properly implement a TKIP protection mechanism, which makes it easier for remote attackers to obtain access to a Wi-Fi network by reading Wi-Fi frames.

CVE-2010-4648 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 3.3 - LOW

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
667907 – (CVE-2010-4648) CVE-2010-4648 kernel: orinoco: fix TKIP countermeasure behaviour	Patch, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=667907
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch, 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=0a54917c3fc295cb61f3fb52373c173fd3b69f48
oss-security - Re: CVE Request: kernel [Re: Security review of 2.6.32.28]	Patch, www.openwall.com, text/html	MLIST [oss-security] 20110106 Re: CVE Request: kernel [Re: Security review of 2.6.32.28]
404 Not Found	ftp.osuosl.org	CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.37

	text/plain Inactive Link Not Archived	
orinoco: fix TKIP countermeasure behaviour · torvalds/linux@0a54917 · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/0a54917c3fc295cb61f3fb52373c173fd3b69f48

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	2.6.36.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.36.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.36.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.36.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.36.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.36.3	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.36.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.36.3:*:*:*:*:*:*:*:

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

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 registred 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