



CVE-2006-5882

Published on: 11/14/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:02 PM UTC

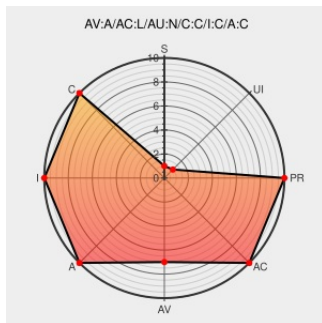
CVE-2006-5882

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Bcmwl5.sys Wireless Device Driver](#) from [Broadcom](#) contain the following vulnerability:

Stack-based buffer overflow in the Broadcom BCMWL5.SYS wireless device driver 3.50.21.10, as used in Cisco Linksys WPC300N Wireless-N Notebook Adapter before 4.100.15.5 and other products, allows remote attackers to execute arbitrary code via an 802.11 response frame containing a long SSID field.

CVE-2006-5882 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **8.3 - HIGH**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Webmail - OVH

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

[VUPEN ADV-2006-4459](#)

US-CERT
Vulnerability Note
VU#209376

[US Government Resource](#)
www.kb.cert.org
[text/html](#)

[CERT-VN VU#209376](#)

Linksys.com
Downloads/Drivers

web.archive.org
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM](#) www.linksys.com/servlet/Satellite?c=L_Download_C2&childpagename=US%2FLayout&cid=1115417109934&packedargs

IBM X-Force
Exchange

exchange.xforce.ibmcloud.com
[text/html](#)

[XF broadcom-bcmwl5-bo\(30202\)](#)

Webmail : Solution

www.vupen.com

[VUPEN ADV-2006-4460](#)

de messagerie professionnelle - OVHcloud- OVH	text/html	
Linksys (A division of Cisco Systems) Information for VU#209376	Patch www.kb.cert.org text/html	 CONFIRM www.kb.cert.org/vuls/id/MAPG-6VGNHW
Broadcom Wireless Driver Probe Response SSID Buffer Overflow - Advisories - Secunia	web.archive.org text/html	 SECUNIA 22831
SecurityTracker.com Archives - Broadcom Wireless Device Driver SSID Buffer Overflow Lets Remote Users Execute Arbitrary Code	securitytracker.com text/html	 SECTrack 1017212
Month of Kernel Bugs (MoKB): Broadcom Wireless Driver Probe Response SSID Overflow	web.archive.org text/html Inactive Link Not Archived	 MISC projects.info-pull.com/mokb/MOKB-11-11-2006.html

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
Hardware  	Broadcom	Bcmwl5.sys Wireless Device Driver	3.50.21.10	All	All	All
Hardware  	Broadcom	Bcmwl5.sys Wireless Device Driver	3.50.21.10	All	All	All
Application	Linksys	Wpc300n Wireless-n Notebook Adapter Driver	All	All	All	All
Application	Linksys	Wpc300n Wireless-n Notebook Adapter Driver	All	All	All	All
cpe:2.3:h:broadcom:bcmwl5.sys_wireless_device_driver:3.50.21.10:*****:						
cpe:2.3:h:broadcom:bcmwl5.sys_wireless_device_driver:3.50.21.10:*****:						
cpe:2.3:a:linksys:wpc300n_wireless-n_notebook_adapter_driver:*****:						
cpe:2.3:a:linksys:wpc300n_wireless-n_notebook_adapter_driver:*****:						

No vendor comments have been submitted for this CVE

© [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](#)