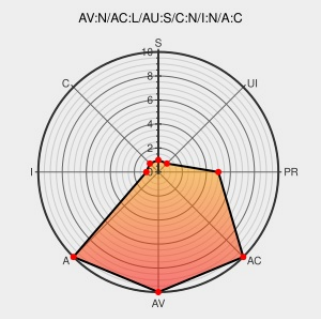
CVE-2007-5475

Published on: 11/12/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:38 PM UTC

CVE-2007-5475

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



Certain versions of Wap4400n from Linksys contain the following vulnerability:

Multiple buffer overflows in the Marvell wireless driver, as used in Linksys WAP4400N Wi-Fi access point with firmware 1.2.17 on the Marvell 88W8361P-BEM1 chipset, and other products, allow remote 802.11-authenticated users to cause a denial of service (wireless access point crash) and possibly execute arbitrary code via an association request with long (1) rates, (2) extended rates, and unspecified other information elements.

CVE-2007-5475 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Linksys WAP4400N Association Request Denial of Service - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	SECUNIA 37345
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20091110 Marvell Driver Multiple Information Element Overflows
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2009-3239

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	Linksys	Wap4400n	1.2.17	All	All	All
Hardware	Linksys	Wap4400n	1.2.17	All	All	All
Hardware	Marvell	88w8361p-bem Chipset	All	All	All	All
Hardware	Marvell	88w8361p-bem Chipset	All	All	All	All

cpe:2.3:h:linksys:wap4400n:1.2.17:*:*:*:*:*:*:*:

cpe:2.3:h:linksys:wap4400n:1.2.17:*:*:*:*:*:*:*:

cpe:2.3:h:marvell:88w8361p-bem_chipset:*:*:*:*:*:*:*:*:

cpe:2.3:h:marvell:88w8361p-bem_chipset:*:*:*:*:*:*:*:*:

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