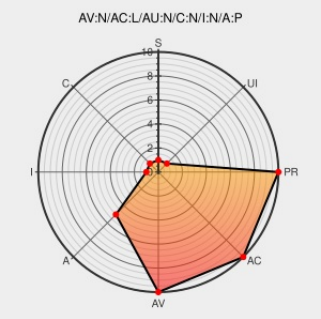
CVE-2005-2585

Published on: 08/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2585

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



Certain versions of Adslfr4ii from Mentor contain the following vulnerability:

Mentor ADSL-FR4II router running firmware 2.00.0111 allows remote attackers to cause a denial of service (active TCP connections state table consumption) via a large number of connections, such as a port scan.

CVE-2005-2585 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
'Low security hole affecting Mentor's ADSLFR4II router' - MARC	marc.info, text/html	BUGTRAQ 20050813 Low security hole affecting Mentor's ADSLFR4II router
Mentor ADSL-FR4II Multiple Vulnerabilities	cve.report (archive), text/html	BID 14557

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	Mentor	Adslfr4ii	2.00.0111	All	All	All
Hardware	Mentor	Adslfr4ii	2.00.0111	All	All	All

cpe:2.3:h:mentor:adslfr4ii:2.00.0111:*:*:*:*:*:*:*:

cpe:2.3:h:mentor:adslfr4ii:2.00.0111:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→