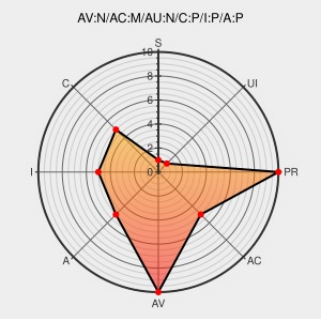
CVE-2013-5730

Published on: 11/19/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:36 PM UTC

CVE-2013-5730

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



Certain versions of Dsl-2740b from Dlink contain the following vulnerability:

Multiple cross-site request forgery (CSRF) vulnerabilities in D-Link DSL-2740B Gateway with firmware EU_1.00 allow remote attackers to hijack the authentication of administrators for requests that (1) enable or disable Wireless MAC Address Filters via a wlFltMode action to wlmacflt.cmd, (2) enable or disable firewall protections via a request to scdmz.cmd, or (3) enable or disable remote management via a save action to scsrvcntr.cmd.

CVE-2013-5730 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
CSRF Exploit	Exploit, www.webapp-security.com, text/html	MISC www.webapp-security.com/wp-content/uploads/2013/09/D-Link-DSL-2740B-Multiple-CSRF-Vulnerabilities1.txt
D-Link DSL-2740B Multiple CSRF Vulnerabilities | CVE-2013-5730 | Ivano Binetti	www.webapp-security.com, text/html	MISC www.webapp-security.com/2013/09/d-link-dsl-2740b-multiple-csrf-vulnerabilities
D-Link DSL-2740B Cross Site Request Forgery ≈ Packet Storm	Exploit, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/123200/D-Link-DSL-2740B-Cross-Site-Request-Forgery.html
D-Link Technical Support	Vendor Advisory, securityadvisories.dlink.com, text/html	CONFIRM securityadvisories.dlink.com/security/publication.aspx?name=SAP10004

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	Dlink	Dsl-2740b	-	All	All	All
Hardware	Dlink	Dsl-2740b	-	All	All	All
Operating System	Dlink	Dsl-2740b Firmware	1.00	All	All	All
Operating System	Dlink	Dsl-2740b Firmware	1.00	All	All	All

cpe:2.3:h:dlink:dsl-2740b:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dsl-2740b:-:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:dsl-2740b_firmware:1.00:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:dsl-2740b_firmware:1.00:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→