

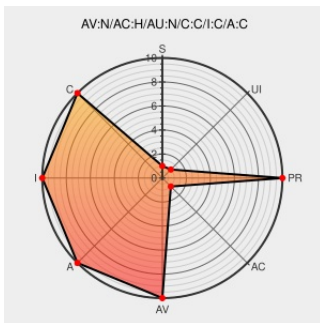


CVE-2013-2271

Published on: 11/15/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:42 PM UTC

CVE-2013-2271

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Dsl-2740b](#) from [Dlink](#) contain the following vulnerability:

The D-Link DSL-2740B Gateway with firmware EU_1.0, when an active administrator session exists, allows remote attackers to bypass authentication and gain administrator access via a request to login.cgi.

CVE-2013-2271 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.6 - HIGH**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

[Exploit](#)
www.webapp-security.com
[text/plain](#)

[MISC](#) www.webapp-security.com/wp-content/uploads/2013/03/D-Link-DSL-2740B-ADSL-Router-Authentication-Bypass2.txt

D-Link Technical Support

[Vendor Advisory](#)
securityadvisories.dlink.com
[text/html](#)

[CONFIRM](#)
securityadvisories.dlink.com/security/publication.aspx?name=SAP10004

D-Link DSL-2740B Authentication Bypass
≈ Packet Storm

[Exploit](#)
packetstormsecurity.com
[text/html](#)

[MISC](#) packetstormsecurity.com/files/120613/dlinkdsl2740b-bypass.txt

D-Link DSL-2740B (ADSL Router)
Authentication Bypass | Ivano Binetti

www.webapp-security.com
[text/html](#)

[MISC](#) www.webapp-security.com/2013/03/d-link-dsl-2740b-adsl-router-authentication-bypass

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

...use of interest to your interest ensure to claim on account of other sites being referenced, or not, from this page. There may be other resources 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	-	All	All	All
Operating System	Dlink	Dsl-2740b Firmware	-	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:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:dlink:dsl-2740b_firmware:-:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)