



- October 12, 2025, 10:17:58 PM
- Welcome, *Guest*

Please [login](#) or [register](#).

 Forever

Login with username, password and session length

News:

This Forum Beta is ONLY for registered owners of D-Link products in the USA for which we have created boards at this time.

- [Home](#)
- [Help](#)
- [Search](#)
- [Login](#)
- [Register](#)
- [D-Link Forums](#) >
- [The Graveyard - Products No Longer Supported](#) >
- [Routers / COVR](#) >
- [DIR-615](#) >
- [Multiple D-Link Router Authentication Bypass Vulnerabilities](#)



« [previous](#) [next](#) »

Pages: [1]

- [Print](#)

Author Topic: Multiple D-Link Router Authentication Bypass Vulnerabilities (Read 46103 times)

[Cartel](#)

- Level 1 Member
- 
- Posts: 13
- 

[Multiple D-Link Router Authentication Bypass Vulnerabilities](#)

« **on:** January 21, 2011, 01:45:19 PM »

Please sticky.

Exploit Title: Multiple D-Link Router Authentication Bypass Vulnerabilities

Date: 12-01-2011

Author: Craig Heffner, /dev/ttyS0

Firmware Link: <http://www.dlink.co.uk/>

Firmware Version(s): All

Tested on: DIR-300, DIR-320, DIR-615 revD

Multiple D-Link routers that use a PHP based Web interface suffer from the same authentication bypass

vulnerability which allows unprivileged users to view and modify administrative router settings.

Further, even if remote administration is disabled this vulnerability can be exploited by a remote

attacker via a CSRF attack.

The vulnerability has been confirmed in the following routers:

DIR-615 revD

DIR-320

DIR-300


The following example URL will allow access to the router's main administrative Web page without authentication:

http://192.168.0.1/bsc_lan.php?NO_NEED_AUTH=1&AUTH_GROUP=0

For a more detailed description of the vulnerability, see: http://www.devttys0.com/wp-content/uploads/2010/12/dlink_php_vulnerability.pdf.

Note that this vulnerability was independently discovered in the DIR-300 and subsequently reported by Karol Celin on 09-Nov-2010 [1].

[1] <http://www.securityfocus.com/archive/1/514687/30/120/threaded>

 Logged

Hard Harry


- Guest




[Re: Multiple D-Link Router Authentication Bypass Vulnerabilities](#)

« **Reply #1 on:** January 21, 2011, 08:05:53 PM »

Correctly me if I am wrong, but wouldnt they need to be connecting to the wireless network to begin with to get a IP and connect to the gateway? So wouldn't wireless security make this a moot point? If someone is trying to bypass your routers password with a wired connection, they can just as easily reset the router to factory with a press of a button.

 Logged

Skello

- Level 3 Member
- 
- Posts: 139
-



Re: Multiple D-Link Router Authentication Bypass Vulnerabilities

« **Reply #2 on:** January 22, 2011, 01:10:42 AM »

[Quote from: Hard Harry on January 21, 2011, 08:05:53 PM](#)

Correctly me if I am wrong, but wouldnt they need to be connecting to the wireless network to begin with to get a IP and connect to the gateway?

No, it is a cross-site request forgery attack (CSRF), which means the attacker uses your browser to perform the attack.

Consider this scenario:

1. There is an URL that allows you to perform operations on the router without the need of logging in (like the one presented above).
2. The attacker crafts such an URL that would enable remote management for the router.
3. He comes to forums.dlink.com and makes a post in the DIR-615 thread with a fictional "need help" story and a link to an outside page, allegedly to some screenshot or whatever. (basically some social engineering to make you click the link)
4. The page on which you land contains an `` HTML tag with a `src=` attribute set as the URL to enable remote management for your router.


At this point your browser will attempt to follow the SRC of the IMG so it can load it, and will therefore query the maliciously crafted URL. Since it doesn't require any authentication, you won't see a thing. It will all happen in the background.

At this point your router accepts remote connections to the interface from the outside world and since there's a authentication bypass vulnerability, he can exploit it directly to do whatever he wants on your device.


It's game over for your security. With control to the router he can mount a man-in-the-middle attack and hijack your sessions for Facebook, email and whatever else he wants.

Scary, but not very useful for mass attacks. It needs to be pretty targeted. But if someone wants to pwn you specifically, then yeah, this offers a nice way to do it.

« *Last Edit: January 22, 2011, 01:12:14 AM by Skello* »

 Logged

Cartel

- Level 1 Member
- 
- Posts: 13
-



[Re: Multiple D-Link Router Authentication Bypass Vulnerabilities](#)

« **Reply #3 on:** January 22, 2011, 11:47:19 AM »

Also check this out:

<http://www.sourcesec.com/2010/01/09/d-link-routers-one-hack-to-own-them-all/>

Quote

January 9th, 2010

We've been on hiatus over the past few months working on other projects, but last week we re-focused on D-Link routers. While we previously found a flaw in D-Link's CAPTCHA implementation, this time around we've found a way to view and edit D-Link router settings without any administrative credentials.

The short story is that D-Link routers have a second administrative interface, which uses the Home Network Administration Protocol. While HNAP does require basic authentication, the mere existence of HNAP on D-Link routers allows attackers and malware to bypass CAPTCHA & security. Further, HNAP authentication is not properly implemented, allowing anyone to view and edit administrative settings on the router.

HNAP appears to have been implemented in D-Link routers since 2006, and cannot be disabled. We have verified that vulnerabilities exist in the HNAP implementations of the DI-524, DIR-628 and DIR-655 routers, and suspect that most, if not all, D-Link routers since 2006 are vulnerable.

<http://www.sourcesec.com/2009/05/12/d-link-captcha-partially-broken/>

Quote

May 12th, 2009

Hack-A-Day reported on D-Link's new captcha system designed to protect against malware that alters DNS settings by logging in to the router using default administrative credentials. I downloaded the new firmware onto our DIR-628 to take a look, and quickly found a flaw in the captcha authentication system that allows an attacker to glean your WiFi WPA pass phrase from the router with only user-level access, and without properly solving the captcha.

When you login with the captcha enabled, the request looks like this:

```
GET /post_login.xml?
hash=c85d324a36fbb6bc88e43ba8d88b10486c9a286a&auth_code=0C52F&auth_id=268D2
```

The hash is a salted MD5 hash of your password, the auth_code is the captcha value that you entered, and the auth_id is unique to the captcha image that you viewed (this presumably allows the router to check the auth_code against the proper captcha image). The problem is that if you leave off the auth_code and auth_id values, some pages in the D-Link Web interface think that you've properly authenticated, as long as you get the hash right:

```
GET /post_login.xml?hash=c85d324a36fbb6bc88e43ba8d88b10486c9a286a
```

Most notably, once you've made the request to post_login.xml, you can activate WPS with the following request:

```
GET /wifisc_add_sta.xml?method=pbutton&wps_ap_ix=0
```

When WPS is activated, anyone within WiFi range can claim to be a valid WPS client and retrieve the WPA passphrase directly from the router.

Further, one need not log in with Administrative credentials to perform this attack; only User-level access is required to activate WPS. This means that even if you load the new firmware on your router, use a strong WPA pass phrase, and change your Administrative login, an attacker can still activate WPS and gain access to your wireless network by simply having an internal client view a Web page.

The attack works like this:

1. Malware loads the router's index page and glean the salt generated by the router.
2. The malware uses the salt to generate a login hash for the D-Link User account (blank password by default).
3. The malware sends the hash to the post_login.xml page.
4. The malware sends a request to the wifisc_add_sta.xml page, activating WPS.
5. The attacker uses WPSpy to detect when the victim's router is looking for WPS clients, and connects to the WiFi network using a WPS-capable network card. Additionally, this vulnerability could be triggered by a simple JavaScript snippet using anti-DNS pinning, which removes the requirement for the attacker to have installed malware onto a machine inside the target network; the victim could be exploited by simply browsing to an infected Web page.

http://viewer.zoho.com/api/urlview.do?url=http://www.sourcesec.com/Lab/dlink_hnap_captcha.pdf


Also someone posted about this a YEAR ago, and nobody said squat.

<http://www.dslreports.com/forum/remark,23623107>

Quote

We have verified that vulnerabilities exist in the HNAP implementations of the DI-524, DIR-628 and DIR-655 routers, **and** suspect that most, if not all, D-Link routers since 2006 are vulnerable

« Last Edit: January 22, 2011, 11:52:09 AM by Cartel »

 Logged

FurryNutz

- Poweruser

-



-



- Posts: 49923



- D-Link Global Forum Moderator

-



Re: Multiple D-Link Router Authentication Bypass Vulnerabilities

« **Reply #4 on:** January 22, 2011, 12:54:34 PM »

Think there would be bigger fish to fry then Jane Doe Or Avg Joe's router. I see a concern of securing the routers. People need to be more aware of what goes on on there routers and who they let on there network and what they click on. People hook up and just forget what goes on behind the scenes. Probably careless about the equipment, just as long as it works. Over all it's

up to everyone to be responsible on what they do.

Besides, this issue has been fixed. Update your FW.

« *Last Edit: November 05, 2012, 11:08:19 AM by FurryNutz* »

 Logged

Cable: 1Gb/50Mb>NetGear CM1200>DIR-882>HP 24pt Gb Switch.

COVR-1202/2202/3902,DIR-2660/80,3xDGL-4500s,DIR-

LX1870,857,835,827,815,890L,880L,868L,836L,810L,685,657,3x655s,645,628,601,DNR-202L,DNS-345,DCS-933L,936L,960L and 8000LH.

- [Print](#)

Pages: [1]

[« previous](#) [next »](#)

- [D-Link Forums](#) >
- [The Graveyard - Products No Longer Supported](#) >
- [Routers / COVR](#) >
- [DIR-615](#) >
- [Multiple D-Link Router Authentication Bypass Vulnerabilities](#)

- [SMF 2.0.13](#) | [SMF © 2016](#), [Simple Machines](#)
- [XHTML](#)
- [RSS](#)
- [WAP2](#)

BlackRain , 2006 by [Crip](#)