D-Link Routers - Authentication Bypass (1)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
15666		CRAIG HEFFNER	WEBAPPS	HARDWARE	2010-12-03

EDB Verified:	Exploit:	Vulnerable App:
✗	{}	

```
# 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
```

Tags:

Advisory/Source: Link