Multiple D-Link Authentication Bypass Vulnerabilities

Craig Heffner
www.devttys0.com

Vulnerability Summary

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.

Affected Products

The vulnerability has been confirmed in the following routers:

- DIR-615 revD
- DIR-320
- DIR-300

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

Vulnerability Description

The affected routers use a PHP based Web interface for administrative management of the device. The Web interface takes advantage of the register_globals feature of PHP to pass and process GET and POST arguments [2].

By default, all pages in the Web interface require authentication, however, certain pages – such as the login page – must be accessed prior to authentication. In order for these pages to opt out of the authentication requirement, they set a PHP variable, NO_NEED_AUTH:

```
<?
/* vi: set sw=4 ts=4: */
$MY_NAME       ="login_fail";
$MY_MSG_FILE=$MY_NAME.".php";

$NO_NEED_AUTH="1";
$NO_SESSION_TIMEOUT="1";
require("/www/model/__html_head.php");
?>
```

The __html_head.php file requires the __auth_check.php file which enforces authentication to the device:

```
<?
/* vi: set sw=4 ts=4: */
if ($NO_NEED_AUTH!="1")
{
        /* for POP up login. */
//      require("/www/auth/__authenticate_p.php");
//      if ($AUTH_RESULT=="401")        {exit;}

        /* for WEB based login  */
        require("/www/auth/__authenticate_s.php");
        if($AUTH_RESULT=="401")         {require("/www/login.php"); exit;}
        if($AUTH_RESULT=="full")        {require("/www/session_full.php"); exit;}
        if($AUTH_RESULT=="timeout")     {require("/www/session_timeout.php"); exit;}

        $AUTH_GROUP=fread("/var/proc/web/session:".$sid."/user/group");
}
require("/www/model/__lang_msg.php");
?>
```

The __auth_check.php script first checks to see if NO_NEED_AUTH has been set to 1. If so, the authentication checks are bypassed completely. Else, it validates that the requesting browser has been successfully authenticated, and sets AUTH_GROUP to the appropriate privilege level (0 for administrator).

However, because the NO_NEED_AUTH and AUTH_GROUP values are not initialized by other administrative pages, they can be set as GET or POST variables thanks to the register_globals PHP feature. By setting NO_NEED_AUTH to 1 and AUTH_GROUP to 0, users can gain administrative access to the router's Web interface.

Proof of Concept

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

Potential For Exploitation

This vulnerability allows anyone with access to the Web interface to view and edit administrative router settings. Further, even if remote administration is disabled on the router, a remote attack can still exploit this vulnerability via a cross site request forgery attack. Since both GET and POST requests are accepted by the router, a simple image tag embedded in an HTML page can be used to change the router's settings as soon as a user inside the local network views the Web page.

Vulnerability Impact

The known affected routers appear to be primarily sold in Europe and Asia, and many can be found via the Shodan search engine [3]. The DIR-615 is perhaps the most notable, as it is the same wireless router distributed to Virgin Media broadband customers, which potentially puts many of their customer networks at risk [4].

It should be noted that other D-Link routers that use PHP based Web interfaces may also be affected.

Mitigations

There are no know mitigations or fixes at the time of this writing.

Disclosure History

17-Jul-2010 Vulnerability discovered
02-Aug-2010 Vendor notified
02-Dec-2010 No response from vendor, vulnerability released

References

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

[2] http://php.net/manual/en/security.globals.php

[3] http://www.shodanhq.com/

[4] http://shop.virginmedia.com/broadband/broadband-extras/wireless-routers.html