

## Re: DLINK 614+ – SOHO routers, system DOS

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-06/0457.html>

---

**From:** Gregory Duchemin (*c3rb3r\_at\_sympatico.ca*)

**Date:** 06/29/04

Date: Mon, 28 Jun 2004 18:27:44 -0700

To: p dont think <pdontthink@angrynerds.com>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hi,

the flaws reported to DLINK on May 24th and posted to bugtraq have been tested on a DI614+ revision A (arm7/2 antennas) firmware 2.30, i have omitted to mention it so please update ...

However:

Rev A's latest firmware available is still 2.30 and therefore IS vulnerable.

<http://support.dlink.com/products/view.asp?productid=DI%2D614%2B>

<http://support.dlink.ca/ProductView.asp?ProdID=220>

for Rev B it seems they have silently released a new firmware 3.41 on June 8

<http://support.dlink.com/products/view.asp?productid=DI%2D614%2B%5FrevB>

<http://support.dlink.ca/ProductView.asp?ProdID=221>

So according to this rep, the flaw was also affecting revision B (as expected) and was fixed on June 8

but in this case, what are they waiting for to patch Rev A ?

Also have you asked him about the script injection issues affecting \_at least\_ their 704 and 614+ rev A and likely several other models ?

Gregory

p dont think wrote:

| FWIW, on a recent call to D-Link tech support, the rep I talked to  
| went to ask someone about it, came back and said that it was an  
| issue that was limited to the 604 and 614 and was fixed in the  
| latest firmware release (sorry, I didn't get a version number). I  
| don't have a 614, so cannot verify.

| – Paul

|  
|  
| TITLE: DLINK 614+ – SOHO routers, system DOS  
| (<http://www.dlink.com>)

| TYPE: ressources starvation / system denial of service

| QUOTE from DLINK:

| The AirPlus DI-614+ combines the latest advancements in 802.11b  
| silicon chip design from Texas Instruments, utilizing their  
| patented Digital Signal Processing™ technology, and D-Link's own  
| robust firewall security features. ... The D-Link AirPlus DI-614+  
| is the ideal networking solution for small offices, home offices,  
| schools, coffee shops and other small businesses that cater to the  
| public.

| DETAILS:

| The DI614+ SOHO router (latest firmware rev 2.30) will automatically  
| reboot when flooded with valid DHCP REQUEST packets built with  
| forged source mac addresses or unique CLIENTID and sent without any  
| REQUESTIP option. Upon reception of this kind of requests, DLINK's  
| DI614+ normally behaves by checking if a lease is available and  
| then reply by offering an ip address along with other network  
| settings as configured through the web base interface. However if  
| such packets are sent at a good enough rate, the DLINK box will be  
| left in an unstable state immediately followed by a system reboot.  
| Timing is quite important here and make me thinking that too much  
| simultaneous requests force the SOHO router to eventually allocate  
| too much memory and thus to reboot. It is actually hard to know  
| with precision where the problem actually lives since no sources  
| are made available for public.

| Note that a reboot will clear any existing lease (as well as logs)  
| and may introduce a subsequent chaos between DHCP clients. Also  
| note that only few seconds are necessary to DOS the box this way,  
| even less time than needed by the system to reboot. So it is a  
| condition of permanent denial of service.

| DLINK 614+ is used, among others, by coffee shops, therefore a  
| successful exploitation may have very disturbing effects.

| EXPLOITATION:

| This bug will NOT be triggered if a REQUESTIP DHCP option is sent  
| along with the request or if no ip address is available for dynamic  
| lease at the time of the attack.

SecurityFocus Bugtraq: Re: DLINK 614+ – SOHO routers, system DOS

| Also for a successful exploitation, packets must be sent at a high  
| enough rate (ie: 50 packets/s is working)

| VENDOR:

| DLINK's support staff has been contacted by May 24th but doesn't  
| bother to reply

| WORKAROUND:

| Use static leasing only and/or disable DLINK's DHCP service

| VULNERABLE:

| firmware up to rev 2.30 (latest)

| AUTHOR: Gregory Duchemin (c3rb3r at sympatico.ca)

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.4 (MingW32)

Comment: Using GnuPG with Mozilla – <http://enigmail.mozdev.org>

iD8DBQFA4MWQ9K2fGbOmSdYRAuKfAJsEDfHL2Gm654LRyZdyZVd2IzU/vACdEhF8  
8pptQuLcKHz+ECgCDvViKhA=  
=/bD/

-----END PGP SIGNATURE-----