

Additional information on WRT54G administration page

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-06/0028.html>

From: Alan W. Rateliff, II (alan2_at_rateliff.net)

Date: 06/02/04

To: <bugtraq@securityfocus.com>

Date: Wed, 2 Jun 2004 14:04:41 -0400

I have made the effort to grab three additional units, all v2 hardware, off-the-shelf, and here is what I have found: Two of three units came with the firewall enabled, while one of the three came with it disabled. The packaging leaves no evidence as to whether any of these items were previously opened and returned.

Interestingly, all three units from local resalers came with v2.02.2 firmware, while the second unit from CDW I tested in March came with v2.02.7. BOTH of the units which came off-the-shelf with v2.02.7 behaved as previously described in my original notice; I do not have records of the firewall setting of the units from March, although they both did behave as predicted after a factory reset.

I would like to assume that the one-of-three v2.02.2 firmware units which came with the firewall disabled was an anomaly, and possibly a customer return. Nicely, flashing these units to v2.02.7 retains all settings, including the firewall status.

Now the catch. In v2.02.7 with the firewall disabled and remote admin turned off, the admin page becomes available on ports 80 and 443 on the WAN. This works whether the unit is in DHCP or PPPoE mode.

Port State Service

80/tcp open http

443/tcp open https

Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20

So part of the original notice is valid, with the exceptions noted. I don't have any more v2.02.2 units to test as they have all now been flashed with v2.02.7, I have no more unmolested v2.02.7, and I am out of petty funds to purchase more :)

So, I will eat some crow on the original notice. To sum up, the admin page is most definitely available to the WAN if the firewall is disabled, regardless of the remote admin setting. And at best the potential for

SecurityFocus Bugtraq: Additional information on WRT54G administration page

getting a unit off-the-shelf with this behavior is somewhat like an Easter egg hunt. I have received an even mix of responses positive and negative to the original notice, so others are reproducing this OTS.

Some thoughts...

It could be reasonable that units which come v2.02.2 OTS then flash to v2.02.7 may not experience this behavior due to stored factory settings from original v2.02.2 system carried over to v2.02.7. That would explain the exception of the OTS behavior of the v2.02.7 units received in March.

Now I am also aware that other LinkSys items I have received have come with firmwares not yet available on the website — most recent example, a WPS54GU2 which came with firmware 6032 while only 6031 was available on the website. It may be more reasonable that since the firmware v2.02.7 is dated March 17, my order for the WRT54G was placed on March 23, maybe a pre-release of the firmware? I cannot imagine that there would be such a diverse distribution of this product direct from LinkSys?

--

```
Alan W. Rateliff, II      : RATELIFF.NET
Independent Technology Consultant : alan2@rateliff.net
(Office) 850/350-0260    : (Mobile) 850/559-0100
```

[System Administration][IT Consulting][Computer Sales/Repair]