

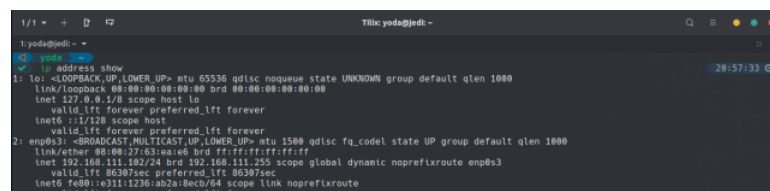
[CVE-2021-37289] A Hidden Web Shell Discovered in the Planex MZK-DP150N Plug-in Wireless LAN Router.

During my last vacation under the sun in Okinawa, I stayed in a beautiful hotel in front of the sea. One day while having my breakfast, I realized that my hotel room was equipped with a small plug-in wireless LAN router from [Planex](#). This device allows a user to share the internet connection of the entire hotel by using a WIFI hotspot for each room. Useful to avoid network spoofing!

After some research on the internet, it was found that Planex is a Japanese brand specializing in routers. I then wondered if these boxes were configured differently from the usual TP-Link, ZTE and other Huawei modems that I am used to using. I then decided to check and see what this Japanese brand has inside!

I took my laptop and connected to the wireless plug-in with the WiFi password kindly given to me by the hotel staff. It was an 8 digit key, which takes less than 10 hours to crack by the way with a brute-force attack... But this is not the topic of this article!

Once connected, I had to know my local IP address and the plug-in wireless Planex IP address in order to connect to the web administration interface.



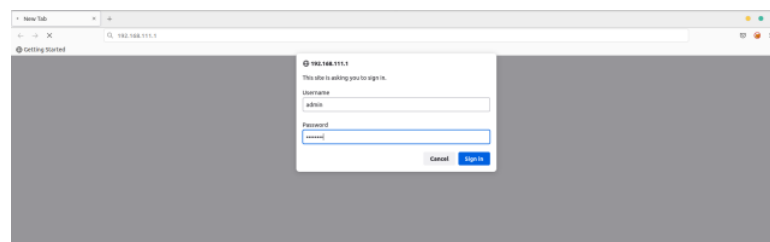
```

1: yoda@yedi: ~
$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:83:ee:ed brd ff:ff:ff:ff:ff:ff
    inet 192.168.111.102/24 brd 192.168.111.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86307sec preferred_lft 86307sec
    inet6 fe80::e311:1236:ab2a:8ecb/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
  
```

— IP address check

192.168.111.1 seems to be the IP address of the web administration interface. Alright I tried to connect, but an .htpasswd was set and asked me for a username and password which I did not have.

I thought it was probably well protected, but I still wanted to try the classic admin:admin default credentials anyways. However, it did not work... so I started to think that I should go and look for the default passwords of Planex devices on the internet. Before i did this though, I wanted to have a last try with the famous combo admin:password... And It worked!



— Boom! We got in! :)

So I finally got inside the web administration interface! The interface seemed to be empty though since there was only 4 buttons displayed. The four buttons displayed were: Change SSID and WIFI password, network settings, update the device by uploading a binary file, and a last button allowing a user to change the .htpasswd that protects the access to the web administration interface.

