Backdoor discovered in PLDT home fiber routers

December 4, 2022 by zux0x3a

Intro

Table of Contents

Last October, I was planning to visit the philippine to get some rest away from work and life pressure. And I would say that was a great direction to relax and enjoy the beauty of nature.
It was a joyful stay, But I was struggling with the quality of the internet, and not always available.

That's not an issue. But I was curious about the security level of IoT devices, especially home Routers. Likely to know more.

Understanding how things work

While reading various resources about home router security and discovering vulnerabilities, I crossed this interesting article shared in 2017 (https://kleo.hak.dog/router-privileged-backdoor-login).

> **Router Privileged Backdoor Login**
>
> Tired of always asking for the WiFi password? Well here in the Philippines, routers come with privileged backdoor login, where we can access the router's configuration, where we

From the first part of the previous blog post, it seems popular that routers came with privileged backdoor login! And That's a security hole by default. Starting from that, I picked up a random/common router (ProLink PLDT home fiber PRS1841 U V2), And I was lucky to spot multiple vulnerabilities and possible attack vectors.

However, I found out that FTP and Telnet are accessible by default, so I tried to access these services using admin/12345 default router credentials. It was authorized but with limited privileges.

But don't have any possible command injection. I also tried to hunt for some RCE in a

web application, but nothing interesting to record.

So I wondered why an admin account doesn't have enough privileges to access Telnet. With quick research across some local philippine community sites. I have found out that PLDT provides a super admin account for high access permission, and the password wasn't hard to retrieve, as a lot was shared on public

However, with the new account "adminpldt / 8d32f84964abbc7a6097e43" I have telnet access with system command execution privileges; I tried to look around for some juicy information, and nothing interesting.
But while retrieving the /etc/passwd. Another account identified as "ADSL" is active by default with an easy password to crack. Honestly, it takes 59 seconds to crack using John, the ripper.

```
# cat passwd
adminpldt:$1$$SPR7qTu3XyYt/KAIBqk5n1:0:0::/tmp:/bin/cli
adsl:$1$$m9g7v7tSyWPyjvelclu6D1:0:0::/tmp:/bin/cli
nobody:x:0:0::/tmp:/dev/null
admin:$1$$iC.dUsGpxNNJGeOm1dFio/:1:0::/tmp:/bin/cli
```

By using "**adsl**" account, I can access both enabled services (Telnet/FTP) with the higher privileges. as the same adminpldt account privileges.

```
================================================================================
                                VDSL Main Menu
================================================================================
(0)  Command mode                 (10) Logout
Enter the option(0-10): 0

Shell command mode
Enter "exit" to exit shell...


# ls -la
drwxr-xr-x   14 adminpld 0              0 Nov  4 23:03 .
drwxr-xr-x   11 502      0            198 Jul 29  2019 ..
-rw-r--r--    1 adminpld 0              6 Nov  4 23:02 TZ
-rw-r--r--    1 adminpld 0             38 Nov  4 23:02 boaSuper.passwd
-rw-r--r--    1 adminpld 0             72 Nov  4 23:02 boaUser.passwd
drwxr-xr-x    2 adminpld 0              0 Nov  6 15:36 config
drwxr-xr-x    3 adminpld 0              0 Jan  1  1970 ct
drwxr-xr-x    2 adminpld 0              0 Jan  1  1970 db
-rw-r--r--    1 adminpld 0             64 Nov  4 23:02 dhcpcV6ptm0_0.conf
-rw-r--r--    1 adminpld 0            793 Nov  4 23:03 dhcpcV6ptm0_0.leases
-rw-r--r--    1 adminpld 0             64 Nov  4 23:02 dhcpcV6vc0.conf
-rw-r--r--    1 adminpld 0              0 Nov  4 23:02 dhcpcV6vc0.leases
-rw-r--r--    1 adminpld 0            186 Nov  4 23:03 dhcpd6.leases
-rw-r--r--    1 adminpld 0              0 Nov  4 23:03 dhcpd6.leases~
-rw-r--r--    1 adminpld 0            279 Nov  4 23:03 dhcpd6_auto.conf
-rw-r--r--    1 adminpld 0             22 Nov  4 23:02 dhcpdMacBase.txt
-rw-r--r--    1 adminpld 0            423 Nov  6 20:19 dnsmasq.conf
drwxr-xr-x    3 adminpld 0              0 Nov  4 23:02 interface
drwxr-xr-x    2 adminpld 0              0 Jan  1  1970 lock
drwxr-xr-x    2 adminpld 0              0 Jan  1  1970 log
drwxr-xr-x    2 adminpld 0              0 Jan  1  1970 mnt
```

Attack Surface

Identifying a backdoor account was helpful to quickly lookup for other devices nearby and see if they were vulnerable. So truly all devices with this module had this silent backdoor account.
The next step is to use Shodan to look up exposed, vulnerable routers, so I tried to search using the router brand or landing page title, but the search was not accurate.

However, while analyzing the Router web server response, I noticed that it is using boa httpd 0.93.15, and an SSL certificate issued by Realtek. By this, I can do a customized search query.

With a country search filter set to Philippine, I counted around 400 exposed devices with FTP access, and more than 3000 were possibly vulnerable to the same attack. With this increasing percentage, there is a possibility for even more vulnerable devices.

A confirmation for an existing backdoor was quick and accurate.

```
331 Password required for adsl.
Password:
230 User adsl logged in.
ftp> dir
200 pcmd command successful.
150 Opening ASCII mode data connection for '/bin/ls'.
-rw-r--r--    1 0            72693 Oct  8 14:40 config.enc
-rw-r--r--    1 0              724 Nov 26 00:05 hosts
-rw-r--r--    1 0                4 Nov 22 08:14 ppp_auth_log
-rw-r--r--    1 0                4 Nov 22 08:14 ppp_diag_log
-rw-r--r--    1 0                1 Nov 22 08:06 ppp_echo_retry
-rw-r--r--    1 0                4 Nov 22 08:14 ppp_error_log
-rw-r--r--    1 0                2 Nov 22 08:06 ppp_lcp_echo
drwxr-xr-x    1 0                0 Oct  8 14:40 ppp_serv_fifo
-rw-r--r--    1 0                4 Nov 22 08:14 ppp_up_log
drwxr-xr-x    1 0                0 Oct  8 14:40 serv_fifo
```

Recommendation

due to the nature of the risk, it is unclear whether PLDT creates the backdoor account or if it is a default setting of the affected router firmware version. It is highly recommended to disable remote/internal access for FTP/SSH. And reset all default passwords for both (admin/adminpldt) accounts. I informed the vendor about the findings but didn't hear back.

Please follow and like us:

zux0x3a

offensive security expert and founder of 0xsp security research and development (SRD),