Advisory ID:	HCA0005 - http://hackingcorp.ch/advisories/HCA0005.pdf
Product:	Horizon HD / WiFi
Vendor:	some Liberty Global plc companies (Unitymedia GmbH, UPC Cablecom, ...)
Affected Version(s):	unknown
Tested Version(s):	current
Vulnerability Type:	Weak WiFi passphrase generation
Risk Level:	Medium
Vendor Notification:	2015-05-14
Public Disclosure:	2016-01-25, patch ready (and validated by HC)
CVE Reference:	Not assigned
Author of Advisory:	Iván Almuiña <ivan.almuina and domain hackingcorp.ch>
Document date:	2015-05-14 initial version sent to Liberty Global plc
Document update:	2016-01-14 censored version for public disclosure
Credits:	Iván Almuiña for finding the vulnerability and developing the Proof-of-Concept
Special Thanks:	Nicolas Oberli for cleaning up the Proof-of-Concept

Description

The current model of the Horizon HD device sold by Liberty Global companies (Unitymedia GmbH, UPC Cablecom, etc. We are not aware of all their companies that sell this Set-Top Box around the world.) uses a weak default SSID/WPA2 passphrase generator. This vulnerability allows an attacker to predict – in a matter of seconds and offline – the default WPA2 passphrase based on the default SSID. By default, the latter is set as UPC24 or UPC50 followed by 7 digits (i.e. UPC241234567).

Technical details

During the boot process the script "/etc/init.d/[redacted]" executes the binary file named "/usr/sbin/[redacted]". This executable checks if it has to setup the default WiFi configuration, the following function manages the process:

Due to legal restrictions and to limit potential damage this information has been removed.

As we can see in the previous excerpt the SSID and WPA2 passphrase generation is based on the Cable Modem MAC address. The [redacted]_* functions are imported from the lib "/lib/[redacted].so" and contains the PRNG algorithm, in the following excerpt we can see that the PRNG is fairly weak:

Due to legal restrictions and to limit potential damage this information has been removed.

Based on the previous information we now know how to bruteforce the key space to find the PRNG's seed, which is the MAC address. An important detail here is that the MAC addresses are 6 bytes long, with the first 3 bytes representing the manufacturer (OUI). This means that we are left with only 3 bytes (24 bits) to bruteforce, greatly reducing the required time to explore all the key space.

The exploit works like this:

- Start with the MAC address [redacted]:00:00:00 until [redacted]:ff:ff:ff
- Generate the SSIDs based on the MAC address and try to match the targeted SSID
- If the SSID matches, generate the passphrase

This process only takes a couple of seconds and has been implemented in a Proof-of-Concept to verify the feasibility of the attack.

Proof of Concept

A weaponized exploit that takes advantage of this vulnerability named 'Horizon-WiFi.c' has been provided to the right persons. The exploit takes a default SSID as input and outputs (in 2-3 seconds) some passphrase candidates, usually between 1 and 4.

If for some reason you consider that you should have access to the exploit and/or the uncensored advisory, feel free to send your demand to 'contact' followed by the domain hackingcorp.ch.

Recommendations

The SSID should not allow to reconstruct the PRNG seed. A solution would be to divert the SSID from a different PRNG and/or use a Cryptographic RNG (CRNG).

For the end users the solution is quite easy, change the default SSID/WPA2 passphrase.

Update 2016/01/14: The new firmware fixes the vulnerability using cryptographic algorithms and diverting the seeds from unpredictable sources. At this point Hacking Corp. does not know if the new firmware has been pushed to all the affected customers, thus we recommend to apply the end users solution previously described.

Disclaimer

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.