# Castlenet Temelli Kablo Modemlerde Kritik WPS Güvenlik Açığı

# Critical WPS Security Vulnerability in Castlenet Based Cable Modems

*Deniz TAŞKIN[1], Cem TAŞKIN[2], İlkay DEMİRALAY[3]*

[1]Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi
Trakya Üniversitesi
deniztaskin@trakya.edu.tr, cemtaskin@trakya.edu.tr

[3]Tunca Meslek Yüksekokulu
Trakya Üniversitesi
ilkaydemiralay@trakya.edu.tr

## Özet

*WPS (wifi protected setup) küçük ofisler ve ev kullanıcıları için 2007 yılında önerilmiş, güvenli kablosuz yerel alan ağını hızlıca kurmaya yönelik bir kimliklendirme seçeneğidir. WPS sayesinde kablosuz ağ güvenliği konusunda bilgisi olmayan son kullanıcılar kolaylıkla yeni bir güvenli kablosuz ağ kurabilmekte, mevcut korunmuş ağa yeni cihazlar ekleyebilmektedir. Her ne kadar WPS, bir kablosuz ağı güvenli bir şekilde yapılandırmayı önerse de günümüzde yapılmış birçok çalışma, tasarımından kaynaklı bazı açıklarından dolayı ağı korumasız bıraktığını göstermektedir. Brute force yolu ile WPS atağının anlatıldığı diğer çalışmalardan farklı olarak bu çalışmada; Castlenet temelli ağ cihazlarında tespit edilen kritik düzeyde nitelendirilebilecek bir güvenlik açığı incelenmekte ve deneysel sonuçlar sunulmaktadır.*

## Abstract

*WPS (WiFi Protected Setup) which have been proposed in 2007 is an authentication option for small office and home users by quickly establishing secure wireless local area network. End-users can easily establish a new secure wireless network, add new devices to the available network with a WPS without knowledge of wireless network security. Although the WPS offers a safe way to setup a secure wireless network, many studies done today show that it leaves the network insecure due to its design. This study differs from other studies which are about brute force attacks to the WPS, as a critical security vulnerability about Castlenet based network devices is examined and experimental results are shown.*

## 1. Giriş

WPS, 2007 yılında Wifi Alliance tarafından son kullanıcı için önerilmiş, güvenli bir ağ kurmanın en kolay yoludur. WPS güvenliği bir kablosuz ağ cihazında: PIN kontrolü, WPS düğmesi, yakın temaslı iletişim ve USB disk sürücüsü metotlarından herhangi birisi kullanılarak sağlanabilmektedir.

Son kullanıcı istediği takdirde bu güvenlik öğelerini devre dışı bırakabilmektedir [1, 2].

2011 yılında Stefan Viehböck tarafından WPS için Brute Force saldırısı temelli bir açık tespit edilmiştir. WPS sisteminde kullanılan PIN anahtarı 8 basamaklıdır. Standart uygulama katmanı PIN anahtarını kullanıcıdan 8 basamak olarak almaktadır. Bu, saldırganın Burte Force atağı için $10^8$ farklı deneme yapmasını gerektirmektedir. Fakat WPS sistemin tasarımı gereği uygulama katmanının altında; PIN anahtarı 4'er basamaktan oluşan iki parça halinde yönlendirici cihaza gönderilmekte ve bu parçalardan herhangi birisi yanlış olduğu takdirde erişim noktası EAP-NACK mesajı geri dönmektedir. Viehböck'e göre EAP-NACK mesajlarının zamanlaması anahtar uzayını $10^8$'den $10^4+10^4$'e düşürmektedir. PIN anahtarına ait ilk blok yanlış olduğu durumda diğer 4 basamaklık bloğu denemeye gerek yoktur. Bunun dışında son PIN basamağının önceki 7 basamağın checksum değeri olması sebebi ile anahtar uzayı $10^4+10^3$'e düşmektedir. Bu açık, atağın gücünü arttırmakta ve çok daha az miktarda deneme yaparak sistem kırılabilmektedir [3].

Viehböck, bu açığın ilgili teknolojiyi kullanan kablosuz ağ cihazlarının tamamında bulunduğunu düşünmekle birlikte; yapmış olduğu çalışma sınırlı sayıda ağ cihazını kapsamaktadır. Gerçekleştirmiş olduğumuz çalışma, WPS sistemini kullanan bazı cihazların Viehböck'in sunmuş olduğundan çok daha kritik açıklara sahip olduğunu göstermektedir.

## 2. Çalışmanın Önemi

Çalışmada anlatılan kritik güvenlik açığı ilk olarak Almanya'da görülmüş olup, servis sağlayıcı tarafından ücretsiz olarak dağıtılmış olan yaklaşık 100.000 adet cihazı etkilediği 2012 yılında tespit edilmiştir. Açığın çıktığı günlerde, servis saylayıcı tarafından açıktan kaçınmanın tek yolunun kablosuz cihaz erişiminin kapatılması yönünde açıklamalar yapılmıştır. Ardından açığı giderecek bir bellenim kullanıcılara sunularak sorun giderilmiştir [4].

2011 yılından itibaren WPS açığından kaçınmaya yönelik birçok güvenlik önlemi ortaya çıkmasına rağmen bazı üreticiler güvenlik konusuna gerekli ciddiyeti hala göstermemektedir. Çalışmayı önemli kılan nokta; ilgili güvenlik açığına sahip cihazların ülkemizde de yüksek

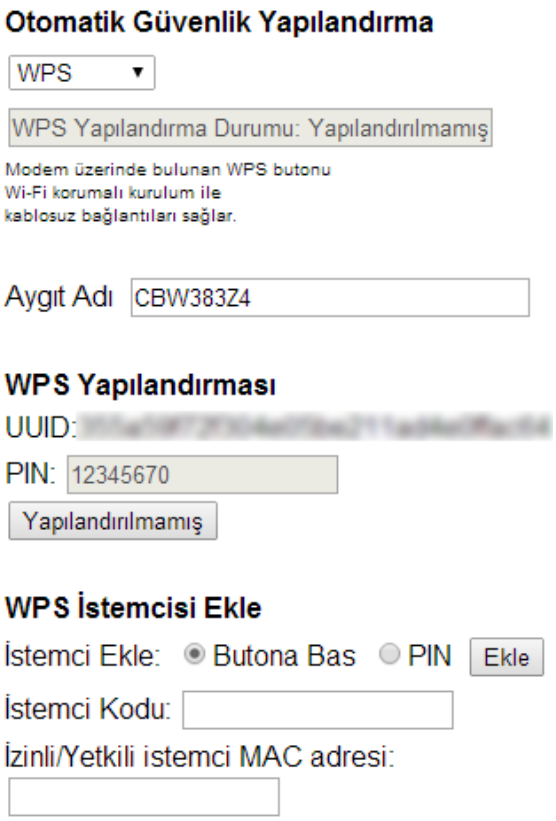
sayılarda aboneye sahip olan bir kablolu internet sağlayıcısı tarafından tek alternatif olarak kullanıcılara sunulması ve ilgili güvenlik açığına sahip bellenimin halen yoğunlukla kullanılıyor olmasıdır.

## 3. Hedef Platform

Çalışmanın konusu güvenlik açığı Castlenet temelli kablosuz ağ cihazlarını içermektedir. Güvenlik açığı olan cihazları MAC adresinin ilk üç byte'lık kısmına bakarak tanımlamak mümkündür. Bu cihazlara ait OUI bilgisi 00-1C-7B şeklindedir. Hedef platform olarak ülkemizde yoğun biçimde kullanılmakta ve kablolu internet sağlayıcısı tarafından abonelere ücretsiz olarak sunulmakta olan Docsis 3.0 standardını destekleyen cihaz seçilmiştir. Hedef platformların çalışmanın yapıldığı tarihteki üretici tarafından sunulmakta olan mp1.799.019 sürüm numaralı bellenimi çalışma kapsamında incelenmiştir. Hedef platforma ait cihazlar PIN anahtarı doğrulama ve WPS düğmesine basılması şeklinde güvenlik özellikleri sunmaktadır.

## 4. Metot

Öncelikle hedef platformlara ait ilgili bellenim cihaza yüklenmektedir. Ardından cihaz fabrika ayarlarına getirilmektedir. Bu durumda; şekil 1'de de görüldüğü gibi varsayılan olarak WPS seçeneği kullanıcıya yapılandırılmamış biçimde sunulmaktadır.




Şekil 1. Hedef cihaza ait yapılandırılmamış WPS seçenekleri

Kullanıcı istediği takdirde WPS özelliğini tamamen kapatabilmesine rağmen, cihazın fabrika ayarlarında bu şekilde gelmesi ve ara yüzde bulunan "yapılandırılmamış" ifadesi, kullanıcıya bu özelliğin kapalı olduğu izlenimini vermektedir. İşletim sistemi seviyesinde incelendiğinde, cihazın WPS özelliğinin görünürde kapalı olarak algılandığı ve WPS PIN anahtarı doğrulama şemasına geçmediği de görülmektedir.

Hedef platformda WPS seçeneği yapılandırılmamış olmasına rağmen, cihaz WPS PIN anahtarı doğrulama saldırısına açıktır. Bu adımdan sonra saldırgan hedef cihaza PIN anahtarı atağı gerçekleştirebilir.

Çalışma kapsamında yapılan atak, cihazın WPS özellikleri yapılandırılmamış olsa dahi varsayılan PIN anahtarı ile kırılması yönündedir. Şekil 2'de de görülmekte olduğu gibi cihaza önermiş olduğumuz saldırı, tek bir anahtarın denenmesi şeklinde uygulandığında yaklaşık 5 saniye içerisinde sistem kırılabilmektedir [5].

```
Waiting for beacon from 00:1C:7B:
Switching mon0 to channel 6
Associated with 00:1C:7B:  (ESSID: NetM  U  net
Trying pin 12345670
Sending EAPOL START request
Received identity request
Sending identity response
Received M1 message
Sending M2 message
Received M3 message
Sending M4 message
Received M5 message
Sending M6 message
Received M7 message
Sending WSC NACK
Sending WSC NACK
Pin cracked in 5 seconds
WPS PIN: '12345670'
WPA PSK: '46  2  2  58e'
AP SSID: 'Net  ER U  net-  '
Nothing done, nothing to save.
```

Şekil 2. WPS PIN atağı

Kullanıcı, ilgili açığı engellemek üzere WPS sistemini yapılandırarak yeni bir PIN anahtarı belirleyebilmektedir. Fakat bu sistemin geleneksel WPS saldırısı ile kırılmasına engel değildir. Viehböck'in önermiş olduğu saldırı ile kablosuz cihazına olan uzaklığa bağlı olarak yaklaşık 4 saat içinde sistem kırılabilmektedir [6].

## 5. Sonuçlar ve Tartışma

Kablosuz ağ cihazları günümüzün vazgeçilmez ağ donanımlarındır. Son kullanıcı marketi incelendiğinde neredeyse tüm kablosuz ağ üreticilerinin WPS sertifikalı cihazlarının bulunduğu görülmektedir. Uzunca bir süredir uzmanlar tarafından bu güvenlik sistemine ait açıklar üzerine çalışmalar yapılmıştır. Yapılan çalışmalar bu sisteme yapılan atakların başarılı sonuçlar verdiği göstermektedir.

Gerçekleştirmiş olduğumuz çalışma göstermektedir ki Castlenet temelli cihazlarda bu açık çok daha tehlikeli bir biçimde yer almaktadır. Ürünler incelendiğinde ilgili üreticinin WPS seçeneklerini uygun biçimde yapılandırmadan pazara sunduğu açıkça görülmektedir. Son kullanıcının ilgili açığı işletim sistemi ve uygulama seviyesinde görme şansı bulunmamaktadır. Hedef cihazların WPS özellikleri üretici tarafından yapılandırılmamış biçimde sunulduğu halde aslında

WPS sistemi kapalı değildir, WPS PIN anahtar atağı için uygundur ve WPS PIN anahtarları "12345670" şeklindedir. Kullanıcı tarafından WEP, WPA veya WPA2 şifreleme metotlarından herhangi birisini kullanması güvenlik açısından bir fark yaratmamaktadır.

Çoğunlukla ev ve küçük ofislerde kullanılan bu tip cihazlar yüzünden kullanıcılar, kişisel maddi kayıpların yanı sıra kendilerinin işlemediği bilişim suçlarıyla da yüzleşmek zorunda kalabilmektedir.

İlgili açığı düzeltmek üzere birçok üretici PIN anahtarının Brute Force yöntemi ile kırılmasını önlemek üzere son kullanıcılara farklı çözümler sunmaktadır. PIN anahtarı deneme sayısını kilitlemek, dahili anahtar girme ekranı sunmak, anahtar deneme aralıklarını uzun tutmak gibi çözümler kullanıcıyı bu ataktan korumaktadır. Ayrıca ataktan korunan cihazlarda WPS özelliğinin tamamen kapatılması da mümkündür.

Bu açılardan değerlendirildiğinde çalışmanın sonuçlarının; kablosuz ağ cihazı üreticileri ve internet servis sağlayıcılarının internet güvenliğine verdikleri önemi arttırmalarına ve madur duruma düşmesi muhtemel son kullanıcıların haklarını korumaya yönelik olduğu görülmektedir.

Bu konuda söylenebilecek diğer bir deneysel sonuç; hedef platform olarak kullanılan Docsis 3.0 özellikli test cihazının kablosuz çekim gücünün çok zayıf olmasıdır. Bu son kullanıcıya bazı sorunlar yaratırken atağı yapacak olan saldırganı cihaza yakın konumda olmaya zorlamaktadır. Bu açıdan bakıldığında saldırganın atak yapmasına zorluk çıkardığı söylenebilir.

## 6. Kaynaklar

[1] http://www.wi-fi.org/wifi-protected-setup

[2] "Frequently Asked Questions: Wi-Fi Protected Setup™". http://www.wi-fi.org/files/WFA Wi-Fi Protectet Setup FAQ.pdf

[3] Vienböch, S. "Brute Force Wi-Fi Protected Setup, When Poor Design Meets Poor Implementation", 2011

[4] http://www.heise.de/netze/meldung/WLAN-Hintertuer-in-Telekom-Routern-1558346.html

[5] reaver-wps, https://code.google.com/p/reaver-wps

[6] Aked, Symon, A. Bolan, C., Murray. B., "A proposed method for examining wireless device vulnerability to brute force attacks via WPS external registrar PIN authentication design", *The 2012 International Conference on Security and Management (SAM'12)*, 2012