

# Air6372S0 Varsayılan Hesap Doğrulaması

written by Mert SARICA | 1 December 2014

15 Kasım Cumartesi sabahı uykulu gözlerle gönderilen tweetlere bakarken Gökmen GÜREŞÇİ'nin "Airties arka kapısını doğrulayabilen oldu mu? Hangi modeller etkileniyor? Ben henüz doğrulayamadım " tweeti ile karşılaştım. Gökmen'e iddianın kaynağını sorduğumda bana Hacker Fantastic Twitter hesabından atılan aşağıdaki tweeti gösterdi.



Bu iddiayı doğrulamak için, IstSec konferansında yaptığım donanım yazılımı analizi sunumuna hazırlanmak için zamanında satın almış olduğum Airties RT-206v4 modeline hızlıca göz atmaya karar verdim. Nmap ile modem bağlantı noktalarını (1-65535) kontrol ettiğimde, modem 2323 bağlantı noktasını dinlemediğini gördüm. Bu durum, bahsedilen varsayılan hesabın sadece belli modellerde geçerli olduğunu ortaya koyuyordu. Elimde başka bir model olmadığı için donanım yazılımını statik olarak analiz etmek için işe koyuldum.

Airties'ın web sitesinde yer alan çoğu kablosuz modem donanım yazılımını

indirdikten sonra donanım yazılım analizi için biçilmiş kaftan olan ve Kali işletim sistemi ile gelen binwalk aracı ile donanım yazılımlarını bu araca toplu bir şekilde analiz ettirmeye başladım.

Destek x  
www.airties.com.tr/support/dcenter/

Air 6372

7/24 destek hattı  
444 0 239

Ürünler / **Kablosuz Ürünler** / Kablosuz DSL ModemAğ Geçitler

Genel Bakış  
Teknik Özellikler  
Sistem Gereksinimleri  
Datashet

**Yükleme merkezi**  
Firmware  
Kolay Kurulum CD'si  
Kullanım Kılavuzu  
Hızlı Kurulum

**AirTies Teknolojileri**

**Ürün Görselleri**

**Destek Dokümanları**

**Satış noktaları**

**Firmware**

1 Ürünü seçiniz Air 6372  
2 Ülkeyi seçiniz Türkiye  
3 Versiyonu seçiniz Superonline

**SON VERSİYON**

Model	Versiyon	Son Güncelleme Tarihi	Açıklama	İndir
Air 6372	1.0.0.42	01.10.2012		

**ÖNCEKİ VERSİYON**

Model	Versiyon	Son Güncelleme Tarihi	Açıklama	İndir
Air 6372	1.0.0.41	30.03.2012		

İlgili ürünler: Air 6271

Kullanım Koşulları | Gizlilik Politikası | Site Haritası | Kariyer

```
Applications Places Thu Nov 20, 1:15 PM root
root@kali: ~/Desktop/Airties
File Edit View Search Terminal Help
root@kali:~/Desktop/Airties# ls *.bin
AirTies_Air5650_FW_1.0.0.10.bin   AirTies_RT-104TT_FW_1.3.0.25.bin
AirTies_Air5650_FW_1.0.0.15.bin   AirTies_RT-204v3_FW_1.0.0.0_FullImage.bin
AirTies_Air5650_FW_1.0.0.5.bin    AirTies_RT-204v3_FW_1.0.0.3_FullImage.bin
AirTies_Air5650v3TT_FW_1.0.2.0.bin AirTies_RT-204v3_FW_1.0.0.5.bin
AirTies_Air6372S0_FW_1.0.0.41.bin  AirTies_RT-204v3KN_FW_1.0.0.8_FullImage.bin
AirTies_Air6372S0_FW_1.0.0.42.bin  AirTies_RT-204v3SM_FW_1.0.0.4_FullImage.bin
AirTies_RT-104_FW_1.0.28.bin       AirTies_RT-206v1TT_FW_3.0.0.13.bin
AirTies_RT-104_FW_1.0.8.bin        AirTies_RT-206v2TT_FW_1.2.0.16.bin
AirTies_RT-104_FW_1.2.0.2.bin      AirTies_RT-206v3TT_FW_1.2.0.18.bin
AirTies_RT-104SM_FW_1.0.31.bin     AirTies_RT-206v3TT_FW_1.2.0.9_FullImage.bin
AirTies_RT-104SM_FW_1.1.17.bin     AirTies_RT-206v4TT_FW_1.2.0.36.bin
AirTies_RT-104TC_FW_1.1.0.6.bin    AirTies_RT-212_FW_1.0.0.3.bin
AirTies_RT-104TT_FW_1.0.26.bin     AirTies_RT-212KN_FW_1.0.0.14.bin
AirTies_RT-104TT_FW_1.0.8.bin      AirTies_RT-212TT_FW_1.2.0.23_FullImage.bin
AirTies_RT-104TT_FW_1.2.0.2.bin
root@kali:~/Desktop/Airties# binwalk -e *.bin
Scan Time:      2014-11-20 13:14:42
Target File:    AirTies_Air5650_FW_1.0.0.10.bin
MD5 Checksum:  541b10e4bf4bf8cf3f11086ef8032049
Signatures:    294
KALI LINUX
the more you are able to hear
DECIMAL        HEXADECIMAL    DESCRIPTION
-----
168            0xA8          uImage header, header size: 64 bytes, header CRC: 0x65458
```

Bilmeyenler için binwalk aracından kısaca bahsetmek gerekirse, bu araç belirtilen donanım yazılımını otomatik olarak analiz ederek eğer sıkıştırılmış (compressed) ise öncelikle açarak içindeki dosyaları, dosya sistemi hiyerarşisine uygun olarak ilgili klasöre kopyalamaktadır. Siz de daha sonra kopyalanan bu dosyaları teker teker inceleyerek donanım yazılımı içinde yer alan yazılımlar, metin belgeleri hakkında fikir sahibi olabilir, konfigürasyon dosyalarını kolaylıkla inceleyebilirsiniz.

binwalk aracına -e parametresi ile tüm donanım yazılımlarını (\*.bin) analiz ettirdikten sonra teker teker her bir açılan klasörün içine bakmak yerine 2323 bağlantı noktasını tüm \*extracted\* geçen (binwalk açtığı donanım yazılımlarını bu şekilde isimlendiriyor) klasör isimleri içinde grep aracı ile aramaya başladım.

```
Applications Places Thu Nov 20, 1:46 PM root
root@kali: ~/Desktop/Airties Bluetooth: On
File Edit View Search Terminal Help
root@kali:~/Desktop/Airties# find *extracted* -type f | xargs grep '2323'
_AirTies_Air6372S0_FW_1.0.0.41.bin-0.extracted/squashfs-root/etc/config.xml:
port>2323</port>
_AirTies_Air6372S0_FW_1.0.0.41.bin-0.extracted/squashfs-root/etc/config.xml:
lan>2323</lan>
_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc/config.xml:
port>2323</port>
_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc/config.xml:
lan>2323</lan>
_AirTies_Air6372S0_FW_1.0.0.42.bin.extracted/squashfs-root/etc/config.xml:
port>2323</port>
_AirTies_Air6372S0_FW_1.0.0.42.bin.extracted/squashfs-root/etc/config.xml:
lan>2323</lan>
root@kali:~/Desktop/Airties#
```

Grep aracının çıktısına göre bu varsayılan hesabın tek bir model için yani Air6372S0 için geçerli olduğu görülmüştü.

config.xml dosyası içinde password kelimesini arattığımda ise iddia edilenden farklı olan SoL\_FiBeR\_1357 şifresi hemen dikkatimi çekti. Bu dosyaya metin editörü ile baktığımda ise bunun root şifresi olduğunu gördüm. (Airties'ın web sitesinde bu model için yer alan donanım yazılımı, Superonline için ayrıca geliştirildiği için muhtemelen şifre farklı)



root@kali: ~/Desktop/\_AirTies\_Air6372S0\_FW\_1.0.0.41.bin.extracted/squashfs-root/etc

File Edit View Search Terminal Help

```
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root# ls
bin etc mnt ramdisk sbin tmp var webs-admin webs.tar.lzma
dev lib proc root sys usr webs webs-guest
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root# cd etc
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc# ls
adsl default_lang filesystems inittab ppp tr069
buildserver defaults.xml fstab mdev.conf rc.d TZ
buildtime device_table.txt gateways miniupnpd resolv.conf wlan
buildversion dproxy.conf group mtab samba
config.xml extract.xml hosts passwd services
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc# gre
p "<password>" *.xml
config.xml: <password>SoL_FiBeR_1357</passw
ord>
config.xml: <password>superonline</password>
config.xml: <password>fiber</password>
config.xml: <password>SoL_FiBeR_1357</passw
ord>
config.xml: <password>superonline</password>
>
config.xml: <password>test</password>
config.xml: <password></password>
defaults.xml: <password>test</password>
defaults.xml: <password>default_password</password>
root@kali:~/Desktop/_AirTies_Air6372S0_FW_1.0.0.41.bin.extracted/squashfs-root/etc#
```

root@kali: ~/Desktop/...

root@kali: ~/Desktop/...





root@kali: ~/Desktop/\_AirTies\_Air6372SO\_FW\_1.0.0.41.bin.extracted/squashfs-root/etc

File Edit View Search Terminal Help

GNU nano 2.2.6 File: config.xml

```
<config version="1.0.1">
  <sysmgr>
    <sysmgr-0>
      <settings>
        <eco0146>1</eco0146>
        <users>
          <user>
            <name>root</name>
            <password>SoL_FiBeR_1357</password>
          </user>
        </users>
      </settings>
    </sysmgr-0>
  </sysmgr>
  <logger>
    <logger-0>
      <log>
        <level>crit</level>
      </log>
      <settings>
        <count>100</count>
      </settings>
    </logger-0>
  </logger>
</config>
```



[ Cancelled ]

^G Get Help    ^O WriteOut    ^R Read File    ^Y Prev Page    ^K Cut Text    ^C Cur Pos  
^X Exit        ^J Justify     ^W Where Is    ^V Next Page    ^U UnCut Text   ^T To Spell

root@kali: ~/Desktop/\_AirTies\_Air6372SO\_FW\_1.0.0.41.bin.extracted/squashfs-root/etc

File Edit View Search Terminal Help

GNU nano 2.2.6 File: config.xml

```
        </settings>
    </ddns-0>
</ddns>
<webui>
    <webui-0>
        <log>
            <level>crit</level>
        </log>
        <settings>
            <users>
                <user>
                    <name>root</name>
                    <enabled>yes</enabled>
                    <password>SoL_FiBeR_1357</password>
                </user>
                <user>
                    <name>admin</name>
                    <enabled>yes</enabled>
                    <password>superonline</password>
                </user>
            </users>
        </settings>
    </webui-0>
</webui>
</ddns-0>
</ddns>
</settings>
```



The quieter you become, the more you are able to hear.

^G Get Help    ^O WriteOut    ^R Read File    ^Y Prev Page    ^K Cut Text    ^C Cur Pos  
^X Exit        ^J Justify     ^W Where Is    ^V Next Page    ^U UnCut Text   ^T To Spell

```
Applications Places Mon Nov 17, 6:32 AM root
root@kali: ~/Desktop/_AirTies_Air6372SO_FW_1.0.0.41.bin.extracted/squashfs-root/etc
File Edit View Search Terminal Help
GNU nano 2.2.6 File: config.xml

<settings>
  <enabled>1</enabled>
  <hostname>Air6372SO</hostname>
  <conns>
    <conn>
      <enabled>1</enabled>
      <name>telnet</name>
      <path>/sbin/telnetd</path>
      <maxconn>1</maxconn>
      <proto>0</proto>
      <port>2323</port>
    </conn>
  </conns>
</settings>
</conn-0>
</conn>
<static>
  <static-0>
    <log>
      <level>crit</level>
    </log>
  </static-0>
</static>

^K Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

root@kali: ~/Desktop/... root@kali: ~/Desktop/...
```

Tabii bende bu marka ve model modem olmadığı için bu kullanıcı adı ve şifrenin doğru olup olmadığını teyit etmek için hemen bir tweet göndererek takipçilerimden yardım istedim ve çok geçmeden hard\_ress Twitter hesabından bu kullanıcı adı ve şifre ile modeme telnet üzerinden bağlanılabildiği bilgisi geldi.

Aslında bunun gibi uzaktan destek amacıyla modemlere, ağ cihazlarına tanımlanan hesaplara ara ara rastlanmakta ve güvenlik araştırmacıları tarafından bunlar ortaya çıkarılmaktadır. Bunların ortaya çıkarılmasının kullanıcılar açısından en önemli kısmı ise, kötüye kullanılabilecek bu şifrelerin en kısa sürede değiştirilebilmesi veya hesapların devre dışı bırakılabilesidir. Bende bunun için iki şifre ile ilgili olarak hemen Netsec e-posta listesine konu ile ilgili bir e-posta göndermeye karar verdim. E-postayı gönderdikten kısa bir süre sonra ise Necati ERSEN ŞİŞECİ'den gelen e-posta beni oldukça şaşırttı. Necati gönderdiği e-postada bu durumu Ocak 2014'de tespit ettiğini ve Superonline ile paylaştığını belirtiyordu (neden Airties değil de Superonline diye soracak olursanız bunun sebebi bu donanım yazılımının Airties firması tarafından Superonline için geliştirilmiş olması) fakat aradan geçen 9 ayda bu konu ile ilgili donanım yazılımında hala



bir düzeltme yapılmamıştı.



N. Ersen SİŞECİ [via](#) netsectr.org  
to liste ▾

10:34 PM (15 hours ago) ☆



Turkish ▾



English ▾

[Translate message](#)

[Turn off for: Turkish](#) ×

Merhaba,

Her iki parolayı da 23 Ocak'da SüperOnline'a bildirmiştim. Uzaktan telnet ile veya root kullanıcı adı ve parolası ile web arayüzünden de girilebiliyor.

Ben bildirdiğim zaman 6372SO için 1.0.0.49 olan sürüm sahada kullanılıyordu. İlk parolayı kendi modemimin yedeğini alıp, içerisinden çıkartmışım. İkinci parolayı ise, Firmware Mod Kit ile çıkartmışım. Her iki yöntemi de SuperOnline'a detaylıca anlatan bir mail atmışım.

SuperOnline, AirTies dan yeni firmware istemişti. AirTies, 1.0.0.52 sürümünü çıkardı ve bu sürümde, (base64 ile encode edilmiş yedekten root şifresi çıkartılmasını diye sanırım) yedek alma özelliği kapatıldı. Bu sürümde yedek alınmıyor. Bu sürüm ile sahadaki bir çok cihaz güncellendi ancak halen daha aynı parolalarla girilebiliyordu. Sanırım şu an hala en güncel sürüm 1.0.0.52.

Defalarca SüperOnline ile maillleştim ancak sonuç ortada. 9 ay oldu.

Umarım bir an önce sahadaki cihazları güncellerler.

Ek bilgi: root kullanıcısı ile web arayüzünden girildiğinde bile menü de olmayan ama TR069 menüsüne <http://ModemIPAdresi/management/tr069.html> adresinden ulaşılabilirsiniz.

İyi geceler.

Necati Ersen ŞİŞECİ

16 Kasım 2014 17:53 tarihinde Mert SARICA <[mert.sarica@gmail.com](mailto:mert.sarica@gmail.com)> yazdı:



Bu tür durumlarda art niyetli kişiler, modemlere uzaktan zararlı yazılım yükleme veya kullanıcıları zararlı sitelere yönlendirme girişiminde bulunabilirler dolayısıyla internet servis sağlayıcısı ve üretici firma tarafından bu tür zafiyetlerin en kısa sürede ortadan kaldırılması gerekmektedir.

Air6372S0 modelini Shodan üzerinde arattığımda ise modem sayısının hiç de azımsanmayacak kadar çok olduğunu (10000+) gördüm.

SHODAN - Computer Search

www.shodanhq.com/search?q=Air6372SO

Like living on the edge? Try out the beta website for Shodan.

Shodan Exploits Scanhub Maps Blog Membership Register Login

SHODAN Air6372SO Search

Results 1 - 10 of about 5727 for Air6372SO

Services	Count	IP Address	Company	Added	Country	Reverse DNS
Telnet (2323)	5,642	176.42.151.7	Superonline ADSL	17.11.2014	Turkey	7.reverse.superonline.net
SMB	58	213.14.140.48	Vestel Elektronik Sanayi ve Ticaret A.S.	17.11.2014	Turkey	48.reverse.superonline.net
NetBIOS	27	91.93.133.76	Global İletişim Hizmetleri A.S.	17.11.2014	Turkey	76.reverse.superonline.net
		176.43.217.211	Superonline ADSL	17.11.2014	Turkey	211.reverse.superonline.net
		78.189.155.33	Turk Telekom	17.11.2014	Turkey	78.189.155.33.static.ttnet.com.tr
		88.250.19.200	Turk Telekom		Turkey	

Hurricane LABS

Celebrating 3 years of Shodan

SHODAN MAPS

Önlem olarak bu marka model modem kullanan kullanıcılara acil olarak port 2323 üzerinden bu şifreler ile modemlerine bağlanıp bağlanamadıklarını kontrol edip root şifrelerini değiştirmeleri gerekmektedir.

Bu hesabın internet servis sağlayıcısı ve üretici firma işbirliği ile en kısa sürede donanım yazılımlarından kaldırılması dileğiyle 2014 yılının bu son yazısı ile 2015 yılının herkese önce sağlık sonra mutluluk getirmesini dilerim.