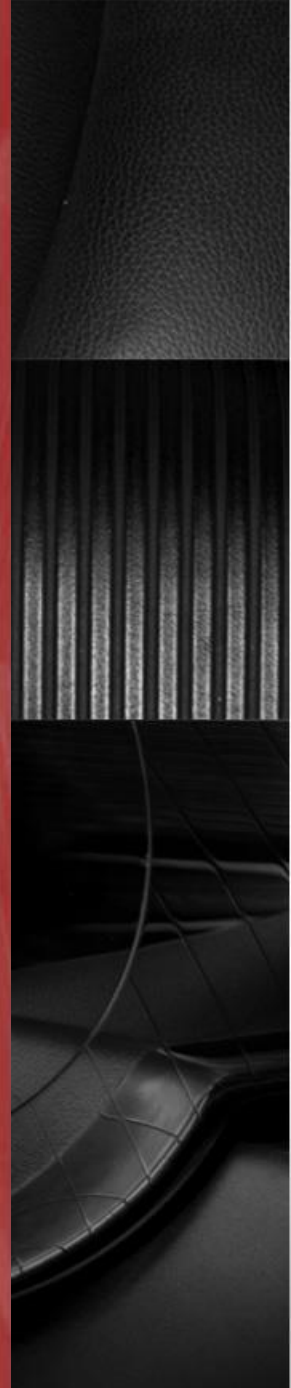


بررسی مودم‌های سری

SWU-3400AN

مهران پارچه بافیه شهریار جلدیری





## مقدمه

- آسیب پذیری های کشف شده
- سناریوهای حمله
- بررسی های بیشتر
- راه کار

# نمونه کارهای پیشین

- حمله به روترهای شرکت Huawei
- ارائه شده در کنفرانس Defcon سال ۲۰۱۲
- ارائه آسیب پذیری های سرریز پشته و هیپ جهت گرفتن دسترسی کامل



**HUAWEI ROUTERS**

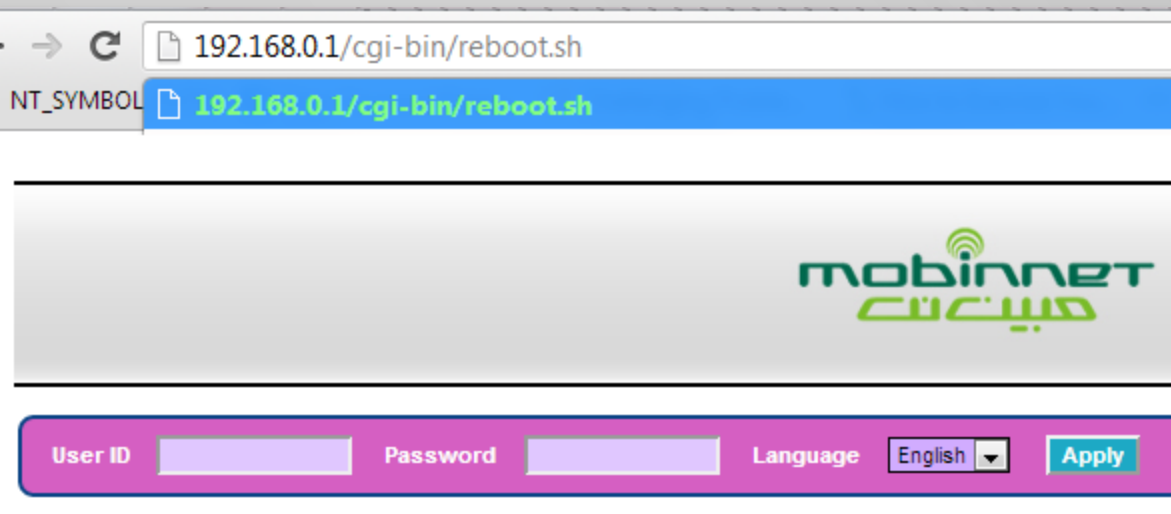
Updated Post-DEFCON XX Version

# آسیب پذیری ها

- راه اندازی مجدد مودم بدون نیاز به احراز هویت
- بارگزاری تمام تنظیمات مودم بدون نیاز به احراز هویت
- مساب کاری پیشفرض غیر مستند
- اجرای دستورات سیستم عامل بدون نیاز به احراز هویت
- سرریز بافر در پشته و اجرای کد مخرب بدون نیاز به احراز هویت
- عدم وجود رمز نگاری در ذخیره سازی داده های حیاتی
- استفاده از نسخه آسیب پذیر Dnsmasq ( نگارش ۲.۴۰ )
- ارسال بسته حاوی SBC-RSP فاص و رد سرویس دهی مودم

# راه اندازی مجدد مودم بدون نیاز به احراز هویت

- راه اندازی مجدد مودم
- عدم نیاز به احراز هویت
- تنظیمات غلط در طراحی سیستم



## بارگزاری تمام تنظیمات مودم بدون نیاز به احراز هویت

- بارگزاری اطلاعات حساس شامل

- نام کاربری و رمز عبور

- رمز عبور Wifi

- و ...

- بدون نیاز به احراز هویت

- تنظیمات غلط در طراحی سیستم

```
1 #The following line must not be removed.
2 Default
3 WebInit=1
4 HostName=mobinnet
5 Login=admin
6 Password=can_you_catch_me?
7 [...]
8 SSID1=Alfie Atkins
9 [...]
10 AuthMode=WPA2PSK
11 EncryptType=AES
12 RekeyInterval=3600
13 RekeyMethod=TIME
14 PMKCachePeriod=10
15 WPAPSK1=secure_password_zzzz
16 DefaultKeyID=2
17 [...]
```

→ 192.168.0.1/cgi-bin/ExportSettings.sh

NT\_SYMBOL



User ID

Password

Language

English

Apply

# حساب کاربری پیشفرض غیر مستند

- نام کاربری و رمز عبور پیشفرض system
- عدم توانایی کاربر Admin جهت شناسایی و یا تغییر رمز عبور

```
.text:004010E4      la      $a1, 0x400000
.text:004010E8      la      $t9, nvram_bufget
.text:004010EC      addiu   $a1, (aLogin - 0x400000) # "Login"
.text:004010F0      jalr    $t9 ; nvram_bufget
.text:004010F4      li      $a0, 1
.text:004010F8      lw      $gp, 0x438+var_428($sp)
.text:004010FC      li      $a0, 1
.text:00401100      la      $a1, 0x400000
.text:00401104      la      $t9, nvram_bufget
.text:00401108      addiu   $a1, (aPassword - 0x400000) # "Password"
.text:0040110C      jalr    $t9 ; nvram_bufget
.text:00401110      move    $s4, $v0
.text:00401114      lw      $gp, 0x438+var_428($sp)
.text:00401118      li      $a0, 1
.text:0040111C      la      $a1, 0x400000
.text:00401120      la      $t9, nvram_bufget
.text:00401124      addiu   $a1, (aLogin1 - 0x400000) # "Login1"
.text:00401128      jalr    $t9 ; nvram_bufget
.text:0040112C      move    $s3, $v0
.text:00401130      lw      $gp, 0x438+var_428($sp)
.text:00401134      li      $a0, 1
.text:00401138      la      $a1, 0x400000
.text:0040113C      la      $t9, nvram_bufget
.text:00401140      addiu   $a1, (aPassword1 - 0x400000) # "Password1"
.text:00401144      jalr    $t9 ; nvram_bufget
```

## اجرای دستورات سیستم عامل بدون نیاز به احراز هویت

- ارسال مستقیم آدرس آی پی به ابزار پینگ
- عدم بررسی صحت داده های ورودی
- توانایی اجرای دستورات سیستم عامل
- عدم نیاز به احراز هویت

```
la      $t9, websGetVar
addiu   $a2, $s4, (asc_456D10+4 - 0x450000)
jalr    $t9 ; websGetVar
addiu   $a1, (aPing_ipaddr - 0x460000) # "ping_ipaddr"
lw      $gp, 0xB8+var_A0($sp)
move    $a0, $s2
la      $a1, 0x460000 |
la      $t9, websGetVar
```



```
addiu   $a1, (aBinPingCSSS2S - 0x460000) # "/bin/ping -c %s %s > %s 2>%s &"
move    $a2, $v0
sw      $s0, 0xB8+var_A4($sp)
sw      $s0, 0xB8+var_A8($sp)
jalr    $t9 ; sprintf
move    $a0, $s1
lw      $gp, 0xB8+var_A0($sp)
nop
la      $t9, doSystem
```



## اجرای دستورات سیستم عامل بدون نیاز به امر از هویت (ادامه)

IP Address (URL)

;  
ls -al

Count

4

```
drwxrwxr-x    2 504      504          0 sbin
drwxr-xr-x    4 504      504          0 lib
drwxrwxr-x   12 504      504          0 etc_ro
lrwxrwxrwx    1 504      504        11 init -> bin/busybox
drwxrwxr-x    7 504      504          0 usr
drwxrwxr-x    2 504      504          0 bin
dr-xr-xr-x   67 0         0          0 proc
drwxr-xr-x   10 0         0          0 sys
drwxr-xr-x    2 0         0          0 tmp
drwxrwxr-x    2 504      504          0 mnt
drwxr-xr-x    3 0         0          0 dev
drwxr-xr-x    4 0         0          0 flash
lrwxrwxrwx    1 504      504          8 etc -> /var/etc
drwxrwxr-x    2 504      504          0 home
drwxr-xr-x    2 0         0          0 media
```

## سرریز بافر در پشته و اجرای کد مخرب بدون نیاز به امراز هویت

- عدم بررسی ورودی ارسالی به وب سرویس
- توانایی سرریز بافر در پشته و اجرای کد های مخرب
- عدم وجود هرگونه محافظت فریب حافظه
- تکرار چند باره آسیب پذیری در نقاط گوناگون

```
move    $a3, $s3
addiu   $a1, (aBinPingCSSS2S - 0x460000) # "/bin/ping -c %s %s > %s 2>%s &"
move    $a2, $v0
sw      $s0, 0xB8+var_A4($sp)
sw      $s0, 0xB8+var_A8($sp)
jalr    $t9, sprintf
move    $a0, $s1
```

# مقدم وجود رمز نگاری در ذخیره سازی داده های حیاتی

- ذخیره سازی تمامی داده ها و تنظیمات به صورت Plain-text

```
84 FragThreshold=2346
85 TxBurst=1
86 PktAggregate=1
87 TurboRate=0
88 WmmCapable=1
89 APAifsn=3;7;1;1
90 APCwmin=4;4;3;2
91 APCwmax=6;10;4;3
92 APTxop=0;0;94;47
93 APACM=0;0;0;0
94 BSSAifsn=3;7;2;2
95 BSSCwmin=4;4;3;2
96 BSSCwmax=10;10;4;3
97 BSSTxop=0;0;94;47
98 BSSACM=0;0;0;0
99 AckPolicy=0;0;0;0
100 APSDCapable=0
101 DLSCapable=0
102 NoForwarding=0
103 NoForwardingBTINBSSID=0
104 HideSSID=0
105 ShortSlot=1
106 AutoChannelSelect=0
107 SecurityMode=0
108 VLANEnable=0
109 VLANName=
110 VLANID=0
111 VLANPriority=0
112 WscConfMode=0
113 WscConfStatus=2
114 WscAKMP=1
115 WscConfigured=0
116 WscModeOption=0
117 WscActionIndex=9
118 WscPinCode=
```

# استفاده از نسخه آسیب پذیر Dnsmasq ( نگارش ۲.۴۰ )

- آسیب پذیری های شناخته شده در نسخه ۲.۴۰
  - آسیب پذیری سرریز بافر در هیپ جهت اجرای کدهای مخرب (CVE-2009-2957)
  - آسیب پذیری Null Pointer Dereference جهت اجرای حمله رد سرویس دهی (CVE-2009-2958)
  - آسیب پذیری رد سرویس دهی با ارسال بسته DNS فاص (CVE-2012-3411)
  - و ...
- عدم نیاز به احراز هویت
- توانایی حمله از طریق اینترنت
  - به طور مثال جهت غیرفعال سازی دیوار آتش

## ارسال بسته حاوی SBC-RSP فاص و رد سرویس دهی مودم

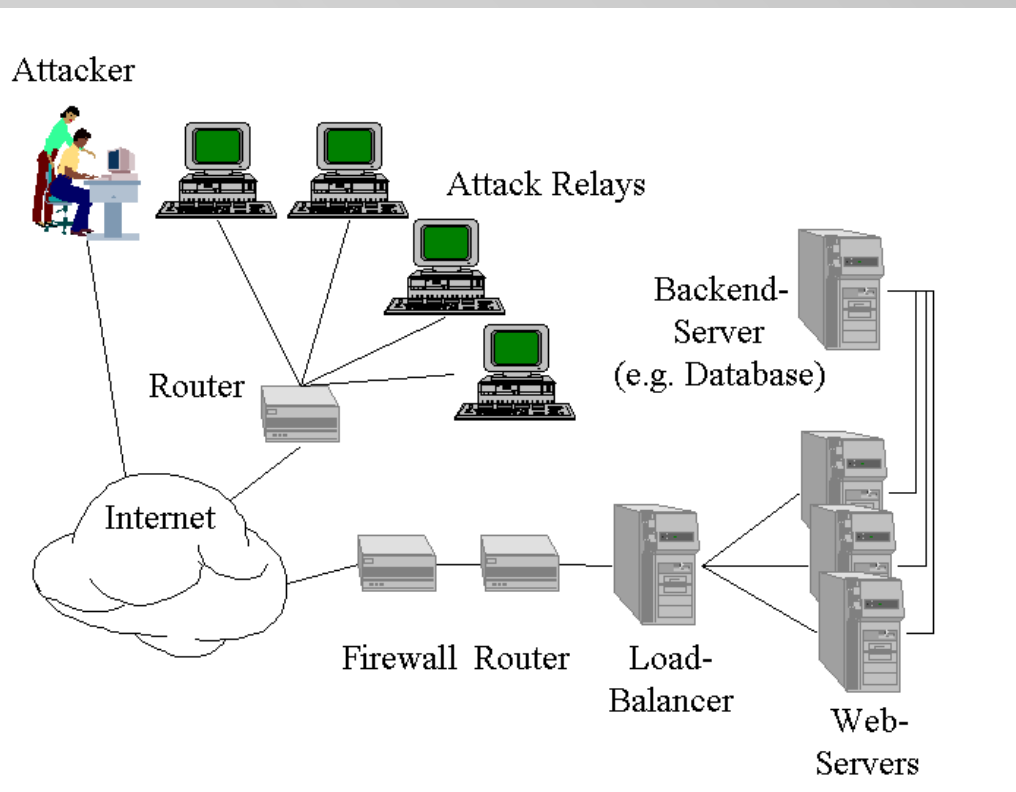
- بررسی پرتوکل MAC
- ارسال بسته های فام و تزریق بسته به صورت Broadcast
- ارسال بسته ی فاص حاوی محتوای SBC-RSP تغییر یافته بر فلاش RFC
- عدم نیاز به اعزاز هویت
- توانایی قطع کامل ارتباط کاربر با مودم ( قطع شبکه )

# سناریوهای حمله (دریافت دسترسی)

- صفحه وب جعلی حاوی کد مخرب جهت :
  - دزدی اطلاعات
  - اجرای دستورات سیستم عامل ( غیرفعال کردن فایروال )
  - اجرای کد مخرب جهت گرفتن دسترسی کامل
  - راه اندازی مجدد مودم
  - و ...
- حمله به ایستگاه های عمومی WiFi ( بدون نیاز به ارتباط با کاربر )
- حمله به Dnsmasq جهت رد سرویس دهی و یا گرفتن دسترسی کامل ( بدون نیاز به ارتباط با کاربر )
- حمله به Dimclient جهت رد سرویس دهی و یا گرفتن دسترسی کامل ( بدون نیاز به ارتباط با کاربر )

# سناریوهای حمله (نفوذ و سوءاستفاده)

- ایجاد شبکه ای از سیستم های آلوده جهت انجام حملات DDOS
- از کار اندازی شبکه های سازمانی



- شنود ترافیک های حیاتی
- تزریق ترافیک (کد مخرب)
- آلوده سازی شبکه (کاربرها)

# کارهای آینده

- بررسی Dnsmasq جهت یافتن آسیب پذیری های ناشناخته
- بررسی Dimclient جهت یافتن آسیب پذیری های ناشناخته

TCP :

```
8096 -> dimclient
9801 -> dimclient
8082 -> dimclient
2002 -> dimclient
53    -> dnsmasq
```

UDP :


```
2048 -> dnsmasq
2049 -> ntpclient
8088 -> dimclient
67    -> udhcpd
53    -> dnsmasq
```





# راه کار

- ارائه آسیب پذیری ها به شرکت سازنده جهت رفع آنها
- گرفتن سورس از شرکت سازنده و رفع آن در داخل
- آموزش به بفش های دافلی (ازجمله بفش فرید)
- مشاوره در زمینه های امنیتی



سوال ؟