

Forum: [Hack Forums](#)

Thread: [An explanation of the windows 7 IPv6 RA Denial of Service Attack](#)

Friedrich Schiller - June 21, 2012, 3:43 am

There is a rather popular post here about a layer 7 denial of service method which directly exploits ipv6 on windows 7 machines.

Original Thread: <https://hackforums.net/showthread.php?tid=2602208>

I recently tested it at home using backtrack and it is everything it lives up to be. There is no doubt of the absolutely amazing raw destructive power inherent in this DoS method.

Here is a video explaining how it works from defcon 19, I HIGHLY recommend you watch this all the way through it is very informative.

[Video: <http://www.youtube.com/watch?v=1EAnjZqXK9E>]

Backtrack 5 has this program automatically built in and is very easily accessed from the terminal. The command is:

```
Code flood_router6 interface  
where interface is wlan0 or eth0 or ath0
```

It seems only cisco has decided to act on this vulnerability by adding RA guards to their switches (don't worry, you can bypass that). The only other clear way of stopping the attack is by turning networking discovery off so that computers do not try to automatically connect to each of the randomly spammed ipv6 prefixes flooding the network. Word has it that microsoft also refuses to patch this problem until the later editions of Windows 8, possibly into Windows 9!

This is a very very dangerous tool, use it with care. I'm actually tempted to try and down an entire internet cafe or library later next week, if I decide to I will post a thread on the forums telling tales of my plunder!

?

Also if anybody can find this style of DoS working over internet (non local) networks PLEASE post some information, I have seen some floating around the net but nothing too informative yet.

Ironsides - June 21, 2012, 6:12 am

Too bad it only works within LAN though.

EmperorDAZ - June 21, 2012, 10:35 am

You can actually load this motherfucker in a mobile phone and wreck computers in that network (as long it's vulnerable, obviously). Simply use an android, install a debian on it, install the required libraries and the thc-ipv6 suite then you're good to go.

This tool actually works because windows and some other vulnerable systems update their routing tables and it seems they tend to consume loads of CPU resource

during the process If I am correct.

Friedrich Schiller - June 21, 2012, 3:30 pm

O.o Wow I know what I'm doing when I have spare time

fred goffa - June 22, 2012, 12:18 am

Thank you for posting this i love to see good matrial posted on hack fuoms

Very nice posted i really enjoyed what u posted up

but its not hard to configur a denial of service attack like this on a external level, i know how to , most attacks through lan can be used on a external level its all how u do it

FastFive - June 22, 2012, 3:38 pm

yo man post a vid if you take out a wireless starbucks or something... that would be cool

Maxitj - June 23, 2012, 7:08 am

(Jun 22, 2012 03:38 PM)FastFive Wrote: [\[CITE\]](#) yo man post a vid if you take out a wireless starbucks or something... that would be cool

Would be hard to shoot ? ...

Friedrich Schiller - June 23, 2012, 3:30 pm

^ Yes it would be, unless I bring a super sneaky hidden camera.

sethyy - June 23, 2012, 5:40 pm

I'd really appreciate a video of this or something...

TickTack - June 23, 2012, 6:50 pm

If you have the balls you should try it on a hospital network. Specifically one where the staff and the visitors use the same public network.

thesnipair.24 - June 23, 2012, 9:50 pm

I think it might work not local only if you open the ports for the network discovery or SMB .. try it .

Friedrich Schiller - June 23, 2012, 11:35 pm

@Tick Tack

Yeah man I so 1337 b4d4zz fo sho' I will nuk3 dem s1ck p33p0l yo.

nerdtopia - August 20, 2014, 3:20 am

do all networks already have an ipv6 address ? If not how would this work