Deeper dive into the recent Windows ICMPv6 vulnerability

Fernando Gont

SI6 NETWORKS

UK IPv6 Council Annual Meeting 2020
December 17th, 2020

What this talk is about

- ICMPv6-based vulnerability found in Windows 10
- An analysis of what went wrong

Introduction

IPv6 Automatic Configuration: Background

- IPv6 has two automatic-configuration mechanisms
- SLAAC [RFC4862] (**mandatory**):
  - Lightweight
  - Allows for all basic network configuration
  - “Anarchic” :-) – every host does what it pleases
- DHCPv6 [RFC8415] (**optional**):
  - Rather heavy-weight
  - Centralized configuration
  - Provides all the configuration knobs you might ever wish for

IPv6 Automatic Configuration: Gaps

- Not really alternative protocols:
  - DHCPv6 cannot provide a default router
  - For many years, SLAAC could not provide a recursive DNS server
- SLAAC support for recursive DNS servers (RDNSS option):
  - RFC5006: Experimental (September 2007)
  - RFC6106: Proposed Standard (November 2010)
  - RFC8106: Proposed Standard (March 2017)

IPv6 Automatic Configuration: Protocol Wars

- Protocol wars at both specification and implementation level:
  - Rejection of standardization of a default router option for DHCPv6
  - For many years, Windows would not support the RDNSS option
  - Android still does not support DHCPv6
- But then:
  - Windows 10 Creators Update (2017!) incorporated support for the RDNSS option
  - Rumor has it that not without some pressure from a big USA-based ISP :-)

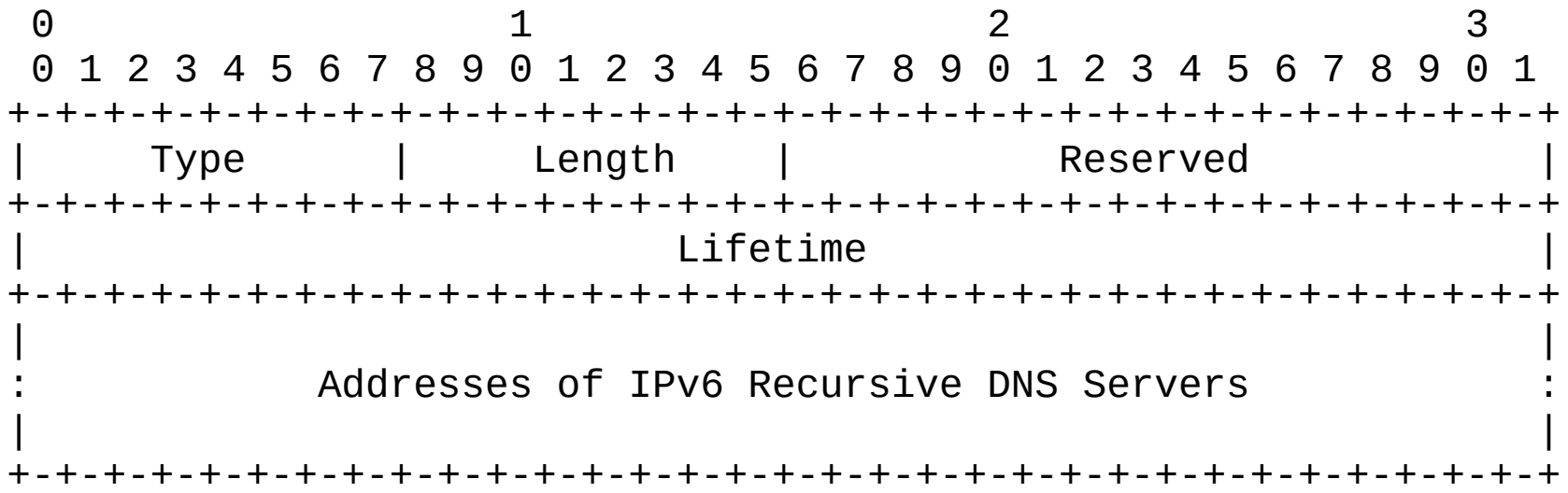
IPv6 Automatic Configuration: What it Means

- RDNSS code is recent, and clearly not well-tested
- (And yes, IPv6 automatic configuration is still a mess)

Windows TCP/IP Remote Code Execution Vulnerability

Recursive DNS Server (RDNSS) Option

- Syntax:



Recursive DNS Server (RDNSS) Option: Checks

- RFC8106, Section 5.3.1. ("Procedure in IPv6 Hosts"):

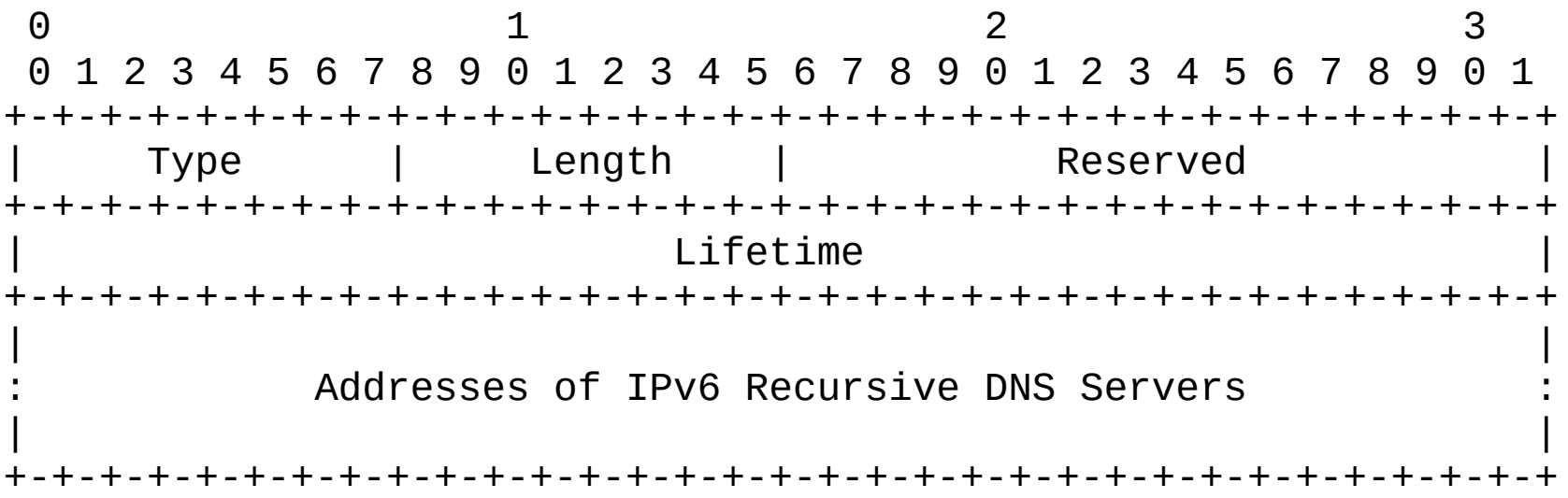
> The validity of DNS options is checked with the Length field; that is, the value of the Length field in the RDNSS option is greater than or equal to the minimum value (3) and satisfies the requirement that **(Length - 1) % 2 == 0**. The value of the Length field in the DNSSL option is greater than or equal to the minimum value (2). Also, the validity of the RDNSS option is checked with the "Addresses of IPv6 Recursive DNS Servers" field; that is, the addresses should be unicast addresses.

Length measured in units of 8 octets. Base option syntax comprising eight octets. One IPv6 address comprising 16 octets (two units of 8 octets)

CVE-2020-16898 Disclosure

- October 13, 2020: Microsoft publishes details on CVE-2020-16898
- [Lots of “I know about the vulnerability, but won’t share details” follow]
- [Some of us tried the obvious, but failed]
- October 16, 2020: **Francisco Falcon** (Quarkslab) and **Adam Zabrocki** (NVIDIA) publish excellent independent analysis

Exploiting the vulnerability (in a nutshell)



- Set Length to even value
- Remaining 8 bytes in the RDNSS option processed as next option

Exploiting the vulnerability (in a nutshell) (II)

- It depends on a lot of Windows 10 packet processing internals
  - The attack packet(s) needs to pass internal validation checks
- Source Address must be link-local
- The packet must all look like a valid packet
- RDNSS option length must be an even number
  - the remaining 8 bytes of the option will be processed as the next Neighbor Discovery option
- The packet needs to be fragmented to pass internal validation checks

Exploiting the vulnerability (in a nutshell) (III)

```
▸ Internet Protocol Version 6, Src: fe80::24f5:a2ff:fe30:8890, Dst: fc00:1::c851:d7c4:5a28:bcbb
▾ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xa263 [unverified] [fragmented datagram]
    [Checksum Status: Unverified]
    Cur hop limit: 0
  ▸ Flags: 0x08, Prf (Default Router Preference): High
    Router lifetime (s): 1800
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ▾ ICMPv6 Option (Recursive DNS Server 4141:4141:4141:4141:4141:4141:4141:4141 4141:4141:4141:4141:4141:4141:4141:4141 4141:4141:4141:4141:1830:ff
      Type: Recursive DNS Server (25)
      Length: 8 (64 bytes)
      Reserved
      Lifetime: Infinity (4294967295)
      Recursive DNS Servers: 4141:4141:4141:4141:4141:4141:4141:4141
      Recursive DNS Servers: 4141:4141:4141:4141:4141:4141:4141:4141
      Recursive DNS Servers: 4141:4141:4141:4141:1830:ff18:18a0:18a0
      Recursive DNS Servers: 18a0:18a0:18a0:18a0:1a01::
  ▾ ICMPv6 Option (RA Flags Extension)
      Type: RA Flags Extension (26)
      Length: 1 (8 bytes)
    ▸ Flags Expansion Option: 0x0000, Prf (Default Router Preference): Medium
      Reserved
  ▾ ICMPv6 Option (Recursive DNS Server aaaa:aaaa:aaaa:aaaa:ffff:aaaa:aaaa:aaaa aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa aaaa:aaaa:aaaa:aaaa:aaaa:aa
      Type: Recursive DNS Server (25)
      Length: 21 (168 bytes)
      Reserved
      Lifetime: Infinity (4294967295)
      Recursive DNS Servers: aaaa:aaaa:aaaa:aaaa:ffff:aaaa:aaaa:aaaa
      Recursive DNS Servers: aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa
      Recursive DNS Servers: aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa
[Unreassembled Packet: ICMPv6]
```


SI6 NETWORKS

Exploiting the vulnerability (in a nutshell) (IV)

No.	Tim	Source	Destination	Protocol	Len	Info
2031	11…	fc00:1::800:27ff:fe00:0	ff02::1:ff28:bcbb	ICMPv6	88	Neighbor Solicitation for fc00:1::c851:d7c4:5a28:bcbb from …
2032	11…	fc00:1::c851:d7c4:5a28:bc…	fc00:1::800:27ff:fe00:0	ICMPv6	88	Neighbor Advertisement fc00:1::c851:d7c4:5a28:bcbb (sol, ov…
2033	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	ICMPv6	216	Router Advertisement[Unreassembled Packet]
2035	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=152 more=y ident=0x2d3c355c nxt=58)
2037	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=304 more=y ident=0x2d3c355c nxt=58)
2042	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=456 more=y ident=0x2d3c355c nxt=58)
2045	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=608 more=y ident=0x2d3c355c nxt=58)
2048	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=760 more=y ident=0x2d3c355c nxt=58)
2049	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=912 more=y ident=0x2d3c355c nxt=58)
2050	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=1064 more=y ident=0x2d3c355c nxt=58)
2051	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=1216 more=y ident=0x2d3c355c nxt=58)
2052	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=1368 more=y ident=0x2d3c355c nxt=58)
2053	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=1520 more=y ident=0x2d3c355c nxt=58)
2054	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	216	IPv6 fragment (off=1672 more=y ident=0x2d3c355c nxt=58)
2055	11…	fe80::24f5:a2ff:fe30:8890	fc00:1::c851:d7c4:5a28:bcbb	IPv6	208	IPv6 fragment (off=1824 more=n ident=0x2d3c355c nxt=58)
2117	11…	0.0.0.0	224.0.0.1	IGMPv2	48	Membership Query, general
2162	12…	10.0.0.129	224.0.0.251	IGMPv2	48	Membership Report group 224.0.0.251
4081	16…	::	ff02::1:ff28:bcbb	ICMPv6	80	Neighbor Solicitation for fe80::c851:d7c4:5a28:bcbb
4082	16…	::	ff02::1:ff28:bcbb	ICMPv6	80	Neighbor Solicitation for fe80::c851:d7c4:5a28:bcbb

What did go wrong?

- Windows failed to validate Router Advertisements and RDNSS options as **required in the very protocol specifications**
- RFC6980, Section 5:

  MUST ignore Router Advertisements that employ fragmentation
- RFC8106, Section 5.3.1:

  *RDNSS valid **if** (Length - 1) % 2 == 0*

Questions?

References

- **Francisco Falcon's analysis:**

  https://blog.quarkslab.com/beware-the-bad-neighbor-analysis-and-poc-of-the-windows-ipv6-router-advertisement-vulnerability-cve-2020-16898.html

- **Adam Zabrocki's analysis:**

  http://blog.pi3.com.pl/?p=780

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com