Zranitelnost měsíce: CVE-2020-16898

Jiří Gogela
Trend Micro Research - DVlabs Praha

Co je „Bad neighbour“?

CVE-2020-16898

Co o tom říká Microsoft...

A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets.
An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client.

To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.

Co je zranitelné?
Windows 10 v.2004, 1903, 1709, 1803, 1909
Windows Server v. 2004, 1903, 1909
Windows Server 2019

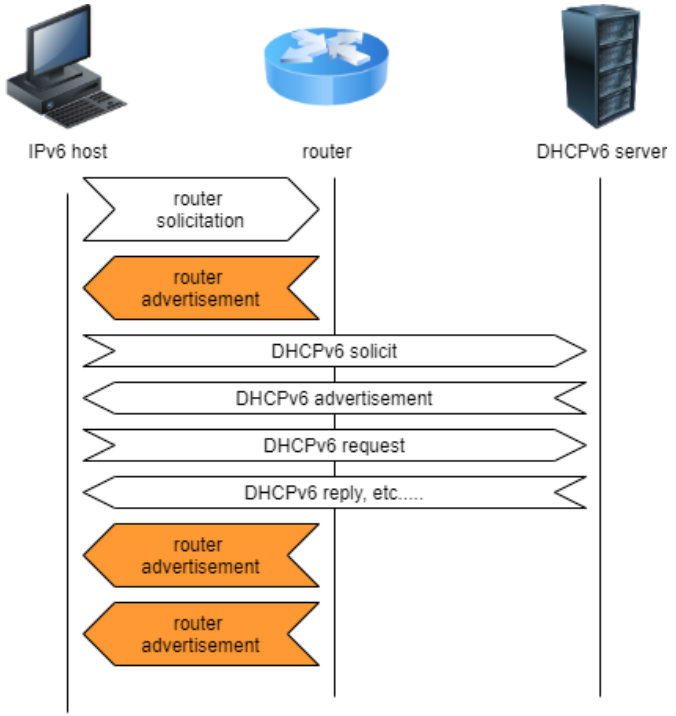
IPV6 je ‘enabled by default’ již od dob od Windows Vista

IPV6, ICMP DHCPv6 a Neighbor Discovery

- IPv6 adresa 128bit

  2001:0db8:0000:0000:0000:8a2e:0370:7334

  Routing prefix(+subnet id) interface identifier
- IPv6 ICMP
- Dynamické přiřazení adresy v IPv6
  - SLAAC / NDP (RFC4861, RFC 8106,...)
  - DHCPv6 (RFC 8415,…)
- RA obsahuje
  - Default route
  - (MTU)
  - (Network prefix)
  - (Recursive DNS Server Option)



IPv6 router advertisment

IPv6 ICMP

Router Adv.

Option type 25
DNS servers

```
0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Type = 134   |     Code      |          Checksum             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                         Reachable Time                        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                          Retrans Timer                        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Options: prefix, MTU,..., RDNSS
 +-+-+-+-+-+-+-+-+-+-+-
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type=25   |     Length    |           Reserved            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                            Lifetime                           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 :            Addresses of IPv6 Recursive DNS Servers            :
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

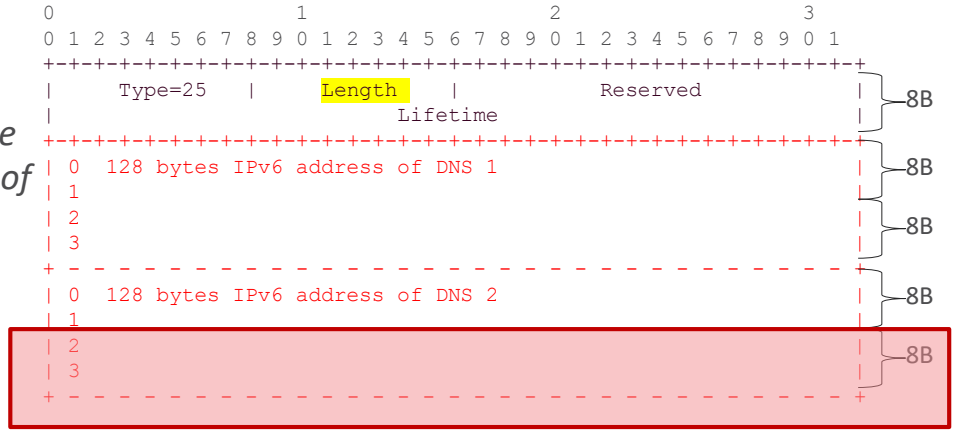
Mechanismus zranitelnosti

Length – délka včetně hlavicky v 8-byte blocích

RFC 8106:

Addresses of IPv6 Recursive DNS Servers One or more 128-bit IPv6 addresses of the RDNSSes. The number of addresses is determined by the Length field. That is, the number of addresses is equal to (Length - 1) / 2.

⇒ hodnota Length musí být vždy **LICHÁ**



Ale co když je náhodou sudá…?

...potřebná délka bufferu se díky celočíselnému dělení spočítá o 8 bytů kratší... Zbývající data se začnou interpretovat jako další Option...

... A nakonec buffer přeteče

Dopad, mechanismus útoku, PoC

- (Momentálně) veřejně dostupné PoC vedou k DoS konkrétní stanice, ale modifikace vedoucí ke spuštění útočníkova kódu není vyloučena.
- Úspěšný útok vyžaduje (kromě výše zmíněné hodnoty v hlavičce) ještě specifickou délku a fragmentaci.
- Útok je možno provádět pouze z lokální sítě.

Zneužití..?

- Lokální síť (?)
- Veřejná wifi
- Malware – momentálně není hlášeno, případný malware by moh překonat LAN gap

Mitigace

- Patch
  - KB4579311
- IPS
  - TippingPoint – 38090
  - Suricata - cve-2020-16898.rules
- RFC 6105 “IPv6 Router Advertisement Guard” (?)
- Segmentace sítě
- Zákaz ICMPv6 RDNSS
  - `netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable`

Reference

- http://blog.pi3.com.pl/?p=780
- https://github.com/0xeb-bp/cve-2020-16898/blob/main/crash.py
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-16898

TREND MICRO™

THE ART OF CYBERSECURITY

Threats detected and blocked globally by Trend Micro in 2018. **Created with real data by artist Daniel Beauchamp.**