

# dnsmasq

## Environmental Information

Ubuntu22.04

dnsmasq-2.91

Network card configuration

Bash

```
1 root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# ifconfig
2 dhcp-test: flags=195<UP,BROADCAST,RUNNING,NOARP> mtu 1500
3     inet 192.168.100.1 netmask 255.255.255.0 broadcast 0.0.0.0
4     inet6 fe80::ece6:eff:feb6:c837 prefixlen 64 scopeid 0x20<link>
5     ether ee:e6:0e:b6:c8:37 txqueuelen 1000 (Ethernet)
6     RX packets 0 bytes 0 (0.0 B)
7     RX errors 0 dropped 0 overruns 0 frame 0
8     TX packets 51536 bytes 17403433 (17.4 MB)
9     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
10
11 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
12     inet 172.17.0.5 netmask 255.255.0.0 broadcast 172.17.255.255
13     ether 36:a7:3d:b9:4e:eb txqueuelen 0 (Ethernet)
14     RX packets 9487524 bytes 9496935139 (9.4 GB)
15     RX errors 0 dropped 0 overruns 0 frame 0
16     TX packets 9167813 bytes 7466589563 (7.4 GB)
17     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
18
19 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
20     inet 127.0.0.1 netmask 255.0.0.0
21     inet6 ::1 prefixlen 128 scopeid 0x10<host>
22     loop txqueuelen 1000 (Local Loopback)
23     RX packets 296956686 bytes 59034980140 (59.0 GB)
24     RX errors 0 dropped 0 overruns 0 frame 0
25     TX packets 296956686 bytes 59034980140 (59.0 GB)
26     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
27
28 vethc: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
29     inet6 fe80::1c1b:beff:fe48:d192 prefixlen 64 scopeid 0x20<link>
30     ether 1e:1b:be:48:d1:92 txqueuelen 1000 (Ethernet)
31     RX packets 594 bytes 83566 (83.5 KB)
32     RX errors 0 dropped 0 overruns 0 frame 0
33     TX packets 165 bytes 19025 (19.0 KB)
34     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
35
36 veths: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
37     inet6 fe80::100d:39ff:feea:5599 prefixlen 64 scopeid 0x20<link>
38     inet6 2001:db8::1 prefixlen 64 scopeid 0x0<global>
39     ether 12:0d:39:ea:55:99 txqueuelen 1000 (Ethernet)
40     RX packets 165 bytes 19025 (19.0 KB)
```

```
41      RX errors 0 dropped 0 overruns 0 frame 0
42      TX packets 594 bytes 83566 (83.5 KB)
43      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

dnsmasq.conf

```
1  interface=dhcp-test
2  bind-interfaces
3
4  port=0
5
6  log-dhcp
7  log-queries
8
9  dhcp-range=2001:db8::100, 2001:db8::200, 64, 12h
10
11  dhcp-option=option6:dns-server,[2001:db8::1]
12
13  dhcp-option=option6:domain-search,example.local
14
15  dhcp-option=option6:ntp-server,[2001:db8::1]
16
17  # 启用路由器通告 ( RA )
18  enable-ra
19
20  # RA参数配置
21  ra-param=dhcp-test,high,0,3600
22
23  # 静态地址分配示例 ( 可选 )
24  # dhcp-host=id:00:01:02:03:04:05,[2001:db8::50],client1
25
26  # 状态文件位置
27  dhcp-leasefile=/var/lib/dhcp/dnsmasq.leases
28
29  # PID文件
30  pid-file=/var/run/dnsmasq.pid
```

YAML

```
tshark -i lo -Y "dhcpv6" -O dhcpv6
```

```
./dnsmasq --no-daemon --log-queries -C ./dnsmasq.conf
```

## Violation Report

### 1. Server Fails to Discard Unicast Solicit Message

```
1  RFC 3315 & RFC8415
2  15. Message Validation
3  A server MUST discard any Solicit, Confirm, Rebind or Information-request messages
   it receives with a unicast destination address.
```

Markdown

According to RFC 3315 & RFC8415, Section 15, "A server **MUST** discard any Solicit... messages it receives with a unicast destination address." The `Solicit` message is intended for discovering available DHCPv6 servers and therefore must be sent to a multicast address.

Our test confirms that `dnsmasq` processes and responds to a `Solicit` message sent directly to its unicast address.

## Reproduce

**Action:** A `Solicit` message was sent directly to the server's unicast address ( `2001:db8::1` ) on port 547.

**Observed Behavior:** The `tshark` capture clearly shows the server at `2001:db8::1` receiving the unicast `Solicit` message (Frame 218) and subsequently responding with an `Advertise` message (Frame 239).

**Expected Behavior:** The server **MUST** have silently discarded the unicast `Solicit` message and sent no response.

```
Bash
1  echo "0155acc300001000e0001000100000000eee60eb6c8370003000c000000010000000000000000
    006000400170018" | xxd -r -p | nc -6u 2001:db8::1 547
```

The server's `Advertise` response is definitive proof of the violation.

```
Bash
1  root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# tshark -i lo -Y "dhcpv6" -O dhcpv6
2  Running as user "root" and group "root". This could be dangerous.
3  Capturing on 'Loopback: lo'
4  ** (tshark:4182782) 14:38:54.972521 [Main MESSAGE] -- Capture started.
5  ** (tshark:4182782) 14:38:54.972564 [Main MESSAGE] -- File: "/tmp/wireshark_loFT
    GC82.pcapng"
6  Frame 218: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interfa
    ce lo, id 0
7  Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00
    (00:00:00:00:00:00)
8  Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
9  User Datagram Protocol, Src Port: 59785, Dst Port: 547
10 DHCPv6
11   Message type: Solicit (1)
12   Transaction ID: 0x55acc3
13   Client Identifier
14     Option: Client Identifier (1)
15     Length: 14
16     DUID: 0001000100000000eee60eb6c837
17     DUID Type: link-layer address plus time (1)
18     Hardware type: Ethernet (1)
19     DUID Time: Jan 1, 2000 00:00:00.000000000 UTC
20     Link-layer address: ee:e6:0e:b6:c8:37
21   Identity Association for Non-temporary Address
22     Option: Identity Association for Non-temporary Address (3)
23     Length: 12
```

```

24         IAID: 00000001
25         T1: 0
26         T2: 0
27     Option Request
28         Option: Option Request (6)
29         Length: 4
30         Requested Option code: DNS recursive name server (23)
31         Requested Option code: Domain Search List (24)
32
33 Frame 239: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on inter
face lo, id 0
34 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00
(00:00:00:00:00:00)
35 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
36 User Datagram Protocol, Src Port: 547, Dst Port: 546
37 DHCPv6
38     Message type: Advertise (2)
39     Transaction ID: 0x55acc3
40     Client Identifier
41         Option: Client Identifier (1)
42         Length: 14
43         DUID: 0001000100000000eeee60eb6c837
44         DUID Type: link-layer address plus time (1)
45         Hardware type: Ethernet (1)
46         DUID Time: Jan 1, 2000 00:00:00.000000000 UTC
47         Link-layer address: ee:e6:0e:b6:c8:37
48     Server Identifier
49         Option: Server Identifier (2)
50         Length: 14
51         DUID: 000100012feeadfb36a73db94eeb
52         DUID Type: link-layer address plus time (1)
53         Hardware type: Ethernet (1)
54         DUID Time: Jun 25, 2025 12:54:19.000000000 UTC
55         Link-layer address: 36:a7:3d:b9:4e:eb
56     Identity Association for Non-temporary Address
57         Option: Identity Association for Non-temporary Address (3)
58         Length: 40
59         IAID: 00000001
60         T1: 21600
61         T2: 37800
62         IA Address
63             Option: IA Address (5)
64             Length: 24
65             IPv6 address: 2001:db8::102
66             Preferred lifetime: 43200
67             Valid lifetime: 43200
68     Status code
69         Option: Status code (13)
70         Length: 9
71         Status Code: Success (0)
72         Status Message: success
73     Preference

```

```

74      Option: Preference (7)
75      Length: 1
76      Pref-value: 0
77      Domain Search List
78      Option: Domain Search List (24)
79      Length: 15
80      Domain name suffix search list
81      List entry: example.local.
82      DNS recursive name server
83      Option: DNS recursive name server (23)
84      Length: 16
85      1 DNS server address: 2001:db8::1
86
87      Frame 240: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits) on inter
face lo, id 0
88      Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00
(00:00:00:00:00:00)
89      Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
90      Internet Control Message Protocol v6
91      DHCPv6
92      Message type: Advertise (2)
93      Transaction ID: 0x55acc3
94      Client Identifier
95      Option: Client Identifier (1)
96      Length: 14
97      DUID: 0001000100000000eeee60eb6c837
98      DUID Type: link-layer address plus time (1)
99      Hardware type: Ethernet (1)
100     DUID Time: Jan 1, 2000 00:00:00.000000000 UTC
101     Link-layer address: ee:e6:0e:b6:c8:37
102     Server Identifier
103     Option: Server Identifier (2)
104     Length: 14
105     DUID: 000100012feeadfb36a73db94eeb
106     DUID Type: link-layer address plus time (1)
107     Hardware type: Ethernet (1)
108     DUID Time: Jun 25, 2025 12:54:19.000000000 UTC
109     Link-layer address: 36:a7:3d:b9:4e:eb
110     Identity Association for Non-temporary Address
111     Option: Identity Association for Non-temporary Address (3)
112     Length: 40
113     IAID: 00000001
114     T1: 21600
115     T2: 37800
116     IA Address
117     Option: IA Address (5)
118     Length: 24
119     IPv6 address: 2001:db8::102
120     Preferred lifetime: 43200
121     Valid lifetime: 43200
122     Status code
123     Option: Status code (13)

```

```

124         Length: 9
125         Status Code: Success (0)
126         Status Message: success
127     Preference
128         Option: Preference (7)
129         Length: 1
130         Pref-value: 0
131     Domain Search List
132         Option: Domain Search List (24)
133         Length: 15
134         Domain name suffix search list
135             List entry: example.local.
136     DNS recursive name server
137         Option: DNS recursive name server (23)
138         Length: 16

```

### 3. Unconditional New Binding Creation on `Rebind`, Leading to Address Pool Exhaustion

According to RFC 8415, Section 18.2.2:

Markdown

```

1 RFC 8415
2 18.3.5. Receipt of Rebind Messages
3 Therefore, the server SHOULD only create new bindings during processing of a Rebind
  message if the server is configured to respond with a Reply message to a Solicit me
  ssage containing the Rapid Commit option.
4

```

Our analysis of the `dnsmasq` source code indicates that the `dhcp6_no_relay` function, which handles the `Rebind` message, does not adhere to this guideline. When the function receives a `Rebind` for a lease that it does not currently have on record, it proceeds to call `lease6_allocate` to create a new binding for the client unconditionally. The implementation is missing the required check of the server's Rapid Commit configuration before creating this new binding.

This means an attacker does not need to go through the normal `Solicit->Advertise->Request->Reply` (SARR) exchange; they can directly trigger a new lease creation simply by sending a `Rebind` message for a lease that does not exist.

**Reproduce:**

Bash

```

1 root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# echo "06dd9a2c0001000e00010001685d3c
  4f0011223344550003002800000001000000000000000000005001820010db8000000000000000000
  1230000003c00000078" | xxd -r -p | nc -6u -q1 2001:db8::1 547

```

Markdown

```

1 Frame 17713: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on inte
  rface lo, id 0
2 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
  0:00:00:00:00:00)

```

```

3  Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
4  User Datagram Protocol, Src Port: 37101, Dst Port: 547
5  DHCPv6
6      Message type: Rebind (6)
7      Transaction ID: 0xdd9a2c
8      Client Identifier
9          Option: Client Identifier (1)
10         Length: 14
11         DUID: 00010001685d3c4f001122334455
12         DUID Type: link-layer address plus time (1)
13         Hardware type: Ethernet (1)
14         DUID Time: Jun 26, 2055 12:25:51.0000000000 UTC
15         Link-layer address: 00:11:22:33:44:55
16     Identity Association for Non-temporary Address
17         Option: Identity Association for Non-temporary Address (3)
18         Length: 40
19         IAID: 00000001
20         T1: 0
21         T2: 0
22         IA Address
23             Option: IA Address (5)
24             Length: 24
25             IPv6 address: 2001:db8::123
26             Preferred lifetime: 60
27             Valid lifetime: 120
28
29  Frame 17813: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on inte
rface lo, id 0
30  Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
0:00:00:00:00:00)
31  Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
32  User Datagram Protocol, Src Port: 547, Dst Port: 546
33  DHCPv6
34      Message type: Reply (7)
35      Transaction ID: 0xdd9a2c
36      Client Identifier
37          Option: Client Identifier (1)
38          Length: 14
39          DUID: 00010001685d3c4f001122334455
40          DUID Type: link-layer address plus time (1)
41          Hardware type: Ethernet (1)
42          DUID Time: Jun 26, 2055 12:25:51.0000000000 UTC
43          Link-layer address: 00:11:22:33:44:55
44      Server Identifier
45          Option: Server Identifier (2)
46          Length: 14
47          DUID: 00010001300a4cd936a73db94eeb
48          DUID Type: link-layer address plus time (1)
49          Hardware type: Ethernet (1)
50          DUID Time: Jul 16, 2025 11:43:21.0000000000 UTC
51          Link-layer address: 36:a7:3d:b9:4e:eb
52      Identity Association for Non-temporary Address

```

```

53      Option: Identity Association for Non-temporary Address (3)
54      Length: 40
55      IAID: 00000001
56      T1: 54
57      T2: 99
58      IA Address
59          Option: IA Address (5)
60          Length: 24
61          IPv6 address: 2001:db8::123
62          Preferred lifetime: 120
63          Valid lifetime: 120
64      NTP Server
65          Option: NTP Server (56)
66          Length: 20
67          NTP Server Address
68              Suboption: NTP Server Address (1)
69              Length: 16
70              NTP Server Address: 2001:db8::1
71      Domain Search List
72          Option: Domain Search List (24)
73          Length: 15
74          Domain name suffix search list
75              List entry: example.local.
76      DNS recursive name server
77          Option: DNS recursive name server (23)
78          Length: 16
79          1 DNS server address: 2001:db8::1

```

Bash

```

1  root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# cat /var/lib/dhcp/dnsmasq.leases
2  duid 00:01:00:01:30:0a:4c:d9:36:a7:3d:b9:4e:eb
3  1752667777 1 2001:db8::123 * * # ->[new]<-
4  1752710104 1 2001:db8::113 * 00:01:00:01:68:5d:0f:51:00:11:22:33:44:55
5  1752709993 1 2001:db8::1e4 * 00:01:00:01:68:5d:0f:41:00:11:22:33:44:55
6  root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src#

```

An attacker can repeatedly send **Rebind** messages with spoofed, unique Client Identifiers (DUIDs). For each malicious **Rebind** packet, **dnsmasq** will incorrectly and unconditionally create a new lease, reserving an IPv6 address from its pool. This process can be repeated until the server's entire address pool is depleted.

Once the address pool is exhausted, legitimate devices on the network will be unable to obtain new leases or renew existing ones, effectively cutting them off from network access and causing a widespread service outage.

## 4. Unconditional Lease Creation Without Configuration Check

Markdown

```

1  RFC 8415
2  18.3.5. Receipt of Rebind Messages

```



3 If the server is configured to create new bindings as a result of processing Rebind messages (also see the note below about the Rapid Commit option (Section 21.14)), the server SHOULD create a binding and return the IA with allocated leases with life times and, if applicable, T1/T2 values and other information requested by the client.

We have observed that when processing Rebind messages, the code unconditionally creates a new lease if an existing lease is not found, without verifying whether the server is configured to allow the creation of new bindings in response to Rebind messages. Consequently, we have classified this behavior as non-compliant. Nevertheless, while this appears to be a minor issue, we have retained the classification to ensure completeness.

## 5. Violation: Ignoring Zero Link-Address Field

## Markdown

```
1 rfc8415
2 13.1. Selecting Addresses for Assignment to an IA_NA
3 According to [RFC6221], the server MUST ignore any link-address field whose value is zero.
```

We have discovered that when handling DHCPv6 relay-forward messages, the code copies the link address field (which may be zero) into the status structure without checking for a zero value. This violates Section 3.1 of RFC6221, which requires that servers must ignore any link address fields with a value of zero.

## Bash

```
1 root@5bfa19bc2f8:~/projects/dnsmasq-2.91/src# echo "0c00000000000000000000000000000000fe8000000000000000000000000000001122fffe3344660009002601a5342e0001000e0001000100000000000011223344660003000c00000000100000000000000000" | xxd -r -p | nc -vu -q1 2001:db8::1 547echo "0c00000000000000000000000000000000fe8000000000000000000000000000001122fffe3344660009002601a5342e0001000e0001000100000000000011223344660003000c000000010000000000000000" | xxd -r -p | nc -vu -q1 2001:db8::1 547
```

## Markdown

```

1  Frame 25386: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on inte
   rface lo, id 0
2  Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
   0:00:00:00:00:00)
3  Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
4  User Datagram Protocol, Src Port: 57034, Dst Port: 547
5  DHCPv6
6      Message type: Relay-forw (12)
7      Hopcount: 0
8      Link address: ::
9      Peer address: fe80::11:22ff:fe33:4466
10     Relay Message
11         Option: Relay Message (9)
12         Length: 38
13         DHCPv6
14             Message type: Solicit (1)
15             Transaction ID: 0xa5342e

```

```

16      Client Identifier
17      Option: Client Identifier (1)
18      Length: 14
19      DUID: 00010001000000000001122334466
20      DUID Type: link-layer address plus time (1)
21      Hardware type: Ethernet (1)
22      DUID Time: Jan  1, 2000 00:00:00.000000000 UTC
23      Link-layer address: 00:11:22:33:44:66
24      Identity Association for Non-temporary Address
25      Option: Identity Association for Non-temporary Address (3)
26      Length: 12
27      IAID: 00000001
28      T1: 0
29      T2: 0

```

As expected, the program should have discarded such messages instead of continuing to process them, but the log:

```

1 dnsmasq-dhcp: no address range available for DHCPv6 request from relay at ::
2 dnsmasq-dhcp: RTR-ADVERT(veths) 2001:db8::

```

Markdown

## 6. Violation in Handling Relay-forward Messages with Hop-Count Limit

```

1 rfc8415
2 19.1.2. Relaying a Message from a Relay Agent
3 If the message received by the relay agent is a Relay-forward message and the hop-count value in the message is greater than or equal to HOP_COUNT_LIMIT, the relay agent discards the received message.
4
5 rfc3315
6 20.1.2. Relaying a Message from a Relay Agent
7 If the message received by the relay agent is a Relay-forward message and the hop-count in the message is greater than or equal to HOP_COUNT_LIMIT, the relay agent discards the received message.

```

Markdown

This issue is small but really very interesting.

The code fails to discard Relay-forward messages when hop-count equals HOP\_COUNT\_LIMIT (32). The rule requires discarding if hop-count  $\geq$  32, but the code only checks for hopcount  $>$  32.

```

2183 /* RFC 3315 HOP_COUNT_LIMIT */
2184 if (hopcount > 32 || !(header = put_opt6(NULL, 34)))
2185     return 1;
2186

```

## 7. Incorrect Use of Interface-Id Option in DHCPv6 Messages

```

1 rfc8415
2 21.18. Interface-Id Option
3 This option MUST NOT appear in any message except a Relay-forward or Relay-reply me
  ssage.
4
5 rfc3315
6 22.18. Interface-Id Option
7 This option MUST NOT appear in any message except a Relay-Forward or Relay-Reply me
  ssage.

```

According to the description of this rule, the Interface-Id Option must not appear in any message other than Relay-forward or Relay-reply. However, when we constructed such messages, the program did not check or reject them.

Bash

```

1 root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# echo "010030390001000e00010001000000
  000011223344550003000c0000000100000000000000000120014746573742d696e746572666163652
  d3132333435" | xxd -r -p | nc -6u -q1 2001:db8::1 547

```

Python

```

1 Frame 30586: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interf
  ace lo, id 0
2 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
  0:00:00:00:00:00)
3 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
4 User Datagram Protocol, Src Port: 34285, Dst Port: 547
5 DHCPv6
6   Message type: Solicit (1)
7   Transaction ID: 0x003039
8   Client Identifier
9     Option: Client Identifier (1)
10    Length: 14
11    DUID: 00010001000000000001122334455
12    DUID Type: link-layer address plus time (1)
13    Hardware type: Ethernet (1)
14    DUID Time: Jan 1, 2000 00:00:00.000000000 UTC
15    Link-layer address: 00:11:22:33:44:55
16   Identity Association for Non-temporary Address
17     Option: Identity Association for Non-temporary Address (3)
18     Length: 12
19     IAID: 00000001
20     T1: 0
21     T2: 0
22   Interface-Id
23     Option: Interface-Id (18)
24     Length: 20
25     Interface-ID: 746573742d696e746572666163652d3132333435
26
27 Frame 30613: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on inte
  rface lo, id 0
28 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0

```

```

0:00:00:00:00:00)
29 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
30 User Datagram Protocol, Src Port: 547, Dst Port: 546
31 DHCPv6
32   Message type: Advertise (2)
33   Transaction ID: 0x003039
34   Client Identifier
35     Option: Client Identifier (1)
36     Length: 14
37     DUID: 00010001000000000001122334455
38     DUID Type: link-layer address plus time (1)
39     Hardware type: Ethernet (1)
40     DUID Time: Jan 1, 2000 00:00:00.000000000 UTC
41     Link-layer address: 00:11:22:33:44:55
42   Server Identifier
43     Option: Server Identifier (2)
44     Length: 14
45     DUID: 00010001300a4cd936a73db94eeb
46     DUID Type: link-layer address plus time (1)
47     Hardware type: Ethernet (1)
48     DUID Time: Jul 16, 2025 11:43:21.000000000 UTC
49     Link-layer address: 36:a7:3d:b9:4e:eb
50   Identity Association for Non-temporary Address
51     Option: Identity Association for Non-temporary Address (3)
52     Length: 40
53     IAID: 00000001
54     T1: 21600
55     T2: 37800
56     IA Address
57       Option: IA Address (5)
58       Length: 24
59       IPv6 address: 2001:db8::1da
60       Preferred lifetime: 43200
61       Valid lifetime: 43200
62   Status code
63     Option: Status code (13)
64     Length: 9
65     Status Code: Success (0)
66     Status Message: success
67   Preference
68     Option: Preference (7)
69     Length: 1
70     Pref-value: 0
71   NTP Server
72     Option: NTP Server (56)
73     Length: 20
74     NTP Server Address
75       Suboption: NTP Server Address (1)
76       Length: 16
77       NTP Server Address: 2001:db8::1
78   Domain Search List
79     Option: Domain Search List (24)

```

```

80      Length: 15
81      Domain name suffix search list
82          List entry: example.local.
83      DNS recursive name server
84      Option: DNS recursive name server (23)
85      Length: 16
86      1 DNS server address: 2001:db8::1

```

## 8. Incorrect Handling of NoAddrsAvail Status Code for IA Option

Markdown

```

1  rfc8415
2  18.3.2. Receipt of Request Messages
3  If the server does not send the NotOnLink status code but it cannot assign any IP a
   ddresses to an IA, the server MUST return the IA option in the Reply message with n
   o addresses in the IA and a Status Code option containing status code NoAddrsAvail
   in the IA.

```

Our analysis reveals that when there are no available addresses in the IA (Identity Association) within a DHCPv6 REQUEST, the server adds a top-level status code option (NoAddrsAvail) instead of embedding it within the IA option as required. According to the specifications, the IA option must include the indication of no available addresses and embed the status code option (NoAddrsAvail) inside the IA itself.

To verify this issue, we first exhausted the address pool of the DHCPv6 server and then sent the request packet.

Bash

```

1  echo "030030390001000e00010001000000000011223344550002000e000100012feeadfb36a73db94
   eeb0003000c00000000100000000000000000000005001820010db80000000000000000000000000000000e10
   00001c20" | xxd -r -p | nc -6u -q1 2001:db8::1 547

```

Markdown

```

1  root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# tshark -i lo -Y "dhcpv6" -O dhcpv6
2  Running as user "root" and group "root". This could be dangerous.
3  Capturing on 'Loopback: lo'
4  ** (tshark:1593669) 06:27:22.152591 [Main MESSAGE] -- Capture started.
5  ** (tshark:1593669) 06:27:22.152641 [Main MESSAGE] -- File: "/tmp/wireshark_loUP
   VR82.pcapng"
6  Frame 84: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interf
   ace lo, id 0
7  Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00
   (00:00:00:00:00:00)
8  Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
9  User Datagram Protocol, Src Port: 56518, Dst Port: 547
10 DHCPv6
11     Message type: Request (3)
12     Transaction ID: 0x003039
13     Client Identifier
14     Option: Client Identifier (1)

```

```

15         Length: 14
16         DUID: 0001000100000000001122334455
17         DUID Type: link-layer address plus time (1)
18         Hardware type: Ethernet (1)
19         DUID Time: Jan  1, 2000 00:00:00.0000000000 UTC
20         Link-layer address: 00:11:22:33:44:55
21     Server Identifier
22         Option: Server Identifier (2)
23         Length: 14
24         DUID: 000100012feeadfb36a73db94eeb
25         DUID Type: link-layer address plus time (1)
26         Hardware type: Ethernet (1)
27         DUID Time: Jun 25, 2025 12:54:19.0000000000 UTC
28         Link-layer address: 36:a7:3d:b9:4e:eb
29     Identity Association for Non-temporary Address
30         Option: Identity Association for Non-temporary Address (3)
31         Length: 12
32         IAID: 00000001
33         T1: 0
34         T2: 0
35     IA Address
36         Option: IA Address (5)
37         Length: 24
38         IPv6 address: 2001:db8::100
39         Preferred lifetime: 3600
40         Valid lifetime: 7200
41
42     Frame 122: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on inter
43     face lo, id 0
44     Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00
45     (00:00:00:00:00:00)
46     Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
47     User Datagram Protocol, Src Port: 547, Dst Port: 546
48     DHCPv6
49         Message type: Reply (7)
50         Transaction ID: 0x003039
51         Client Identifier
52             Option: Client Identifier (1)
53             Length: 14
54             DUID: 0001000100000000001122334455
55             DUID Type: link-layer address plus time (1)
56             Hardware type: Ethernet (1)
57             DUID Time: Jan  1, 2000 00:00:00.0000000000 UTC
58             Link-layer address: 00:11:22:33:44:55
59         Server Identifier
60             Option: Server Identifier (2)
61             Length: 14
62             DUID: 000100012feeadfb36a73db94eeb
63             DUID Type: link-layer address plus time (1)
64             Hardware type: Ethernet (1)
65             DUID Time: Jun 25, 2025 12:54:19.0000000000 UTC
66             Link-layer address: 36:a7:3d:b9:4e:eb

```

```

65     Identity Association for Non-temporary Address
66         Option: Identity Association for Non-temporary Address (3)
67         Length: 37
68         IAID: 00000001
69         T1: infinity
70         T2: infinity
71         Status code
72             Option: Status code (13)
73             Length: 21
74             Status Code: NoAddrAvail (2)
75             Status Message: address unavailable
76     Status code
77         Option: Status code (13)
78         Length: 9
79         Status Code: Success (0)
80         Status Message: success
81     Preference
82         Option: Preference (7)
83         Length: 1
84         Pref-value: 0
85     NTP Server
86         Option: NTP Server (56)
87         Length: 20
88         NTP Server Address
89             Suboption: NTP Server Address (1)
90             Length: 16
91             NTP Server Address: 2001:db8::1
92     Domain Search List
93         Option: Domain Search List (24)
94         Length: 15
95         Domain name suffix search list
96             List entry: example.local.
97     DNS recursive name server
98         Option: DNS recursive name server (23)
99         Length: 16

```

## 9. Missing Requested Options When No Addresses Are Available

纯文本

- 1 rfc8415
- 2 18.3.9. Creation of Advertise Messages
- 3 The server MUST include options in the Advertise message containing configuration parameters for all of the options identified in the Option Request option (see Section 21.7) in the Solicit message that the server has been configured to return to the client.

We found that the server does not include requested options in the Advertise message when no addresses are available. The rule mandates that the server MUST include all requested options

(from the Option Request option in the Solicit) that it is configured to return, regardless of address assignment status.

We constructed a Solicit message explicitly requesting the DNS recursive name server (Option 23) and the domain search list (Option 24). However, in the Advertise message, these options were not included; only the client identifier, server identifier, and the status code "NoAddrAvail" were returned. This indicates that the server was unable to allocate an address and did not provide the requested option content.

## Bash

```
1 root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# echo "010030390001000e00010001000000
000011223344550003000c000000001000000000000000000000060004000170018" | xxd -r -p | nc -6
u -q1 2001:db8::1 547
```

## Markdown

```

1 root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# tshark -i lo -Y "dhcpv6" -O dhcpv6
2 Running as user "root" and group "root". This could be dangerous.
3 Capturing on 'Loopback: lo'
4 ** (tshark:1613859) 06:40:21.568514 [Main MESSAGE] -- Capture started.
5 ** (tshark:1613859) 06:40:21.568556 [Main MESSAGE] -- File: "/tmp/wireshark_lo77F
I82.pcapng"
6 Frame 60: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface
lo, id 0
7 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
0:00:00:00:00:00)
8 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
9 User Datagram Protocol, Src Port: 51651, Dst Port: 547
10 DHCPv6
11     Message type: Solicit (1)
12     Transaction ID: 0x003039
13     Client Identifier
14         Option: Client Identifier (1)
15         Length: 14
16         DUID: 00010000100000000000001122334455
17         DUID Type: link-layer address plus time (1)
18         Hardware type: Ethernet (1)
19         DUID Time: Jan  1, 2000 00:00:00.0000000000 UTC
20         Link-layer address: 00:11:22:33:44:55
21     Identity Association for Non-temporary Address
22         Option: Identity Association for Non-temporary Address (3)
23         Length: 12
24         IAID: 00000001
25         T1: 0
26         T2: 0
27     Option Request
28         Option: Option Request (6)
29         Length: 4
30         Requested Option code: DNS recursive name server (23)
31         Requested Option code: Domain Search List (24)
32
33 Frame 106: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interf
ace lo, id 0

```



```

34 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
   0:00:00:00:00:00)
35 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
36 User Datagram Protocol, Src Port: 547, Dst Port: 546
37 DHCPv6
38     Message type: Advertise (2)
39     Transaction ID: 0x003039
40     Client Identifier
41         Option: Client Identifier (1)
42         Length: 14
43         DUID: 000100010000000000001122334455
44         DUID Type: link-layer address plus time (1)
45         Hardware type: Ethernet (1)
46         DUID Time: Jan  1, 2000 00:00:00.0000000000 UTC
47         Link-layer address: 00:11:22:33:44:55
48     Server Identifier
49         Option: Server Identifier (2)
50         Length: 14
51         DUID: 000100012feeadfb36a73db94eeb
52         DUID Type: link-layer address plus time (1)
53         Hardware type: Ethernet (1)
54         DUID Time: Jun 25, 2025 12:54:19.0000000000 UTC
55         Link-layer address: 36:a7:3d:b9:4e:eb
56     Status code
57         Option: Status code (13)
58         Length: 24
59         Status Code: NoAddrAvail (2)
60         Status Message: no addresses available

```

## 10. Violation of DHCPv6 IA\_PD Handling in Advertise Messages

Markdown

```

1  rfc8415
2  18.3.9.  Creation of Advertise Messages
3  The server MUST include IA options in the Advertise message containing any addresse
   s and/or delegated prefixes that would be assigned to IAs contained in the Solicit
   message from the client.
4
5  rfc3315
6  17.2.2. Creation and Transmission of Advertise Messages
7  If the Solicit message from the client included one or more IA options, the server
   MUST include IA options in the Advertise message containing any addresses that woul
   d be assigned to IAs contained in the Solicit message from the client.

```

We found that dnsmasq does not handle the IA\_PD option in request messages. This is because only IA\_NA and IA\_TA are processed in the `check_ia` function, which explicitly filters out the IA\_PD option (OPTION6\_IA\_PD). As a result, when constructing the Advertise message, the IA\_PD option in the request message is ignored, which violates relevant rules.

C

```

1 static int check_ia(struct state *state, void *opt, void **endp, void **ia_option)
2 {
3     state->ia_type = opt6_type(opt);
4     *ia_option = NULL;
5
6     if (state->ia_type != OPTION6_IA_NA && state->ia_type != OPTION6_IA_TA)
7         return 0;
8
9     if (state->ia_type == OPTION6_IA_NA && opt6_len(opt) < 12)
10        return 0;
11
12    if (state->ia_type == OPTION6_IA_TA && opt6_len(opt) < 4)
13        return 0;
14
15    *endp = opt6_ptr(opt, opt6_len(opt));
16    state->iaid = opt6_uint(opt, 0, 4);
17    *ia_option = opt6_find(opt6_ptr(opt, state->ia_type == OPTION6_IA_NA ? 12 : 4),
18    *endp, OPTION6_IAADDR, 24);
19
20    return 1;
21 }

```

We constructed a Solicit message that includes an IA\_PD option, but the server did not return an Advertise that contains IA\_PD.

Bash

```

1 root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# echo "011718020001000e0000100010000000
00eee60eb6c8370019000c000000010000000000000000" | xxd -r -p | nc -6u -q1 2001:db8::
1 547

```

纯文本

```

1 Frame 40917: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interf
ace lo, id 0
2 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
0:00:00:00:00:00)
3 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
4 User Datagram Protocol, Src Port: 45731, Dst Port: 547
5 DHCPv6
6     Message type: Solicit (1)
7     Transaction ID: 0x171802
8     Client Identifier
9         Option: Client Identifier (1)
10        Length: 14
11        DUID: 0001000100000000eee60eb6c837
12        DUID Type: link-layer address plus time (1)
13        Hardware type: Ethernet (1)
14        DUID Time: Jan  1, 2000 00:00:00.000000000 UTC
15        Link-layer address: ee:e6:0e:b6:c8:37
16    Identity Association for Prefix Delegation
17        Option: Identity Association for Prefix Delegation (25)
18        Length: 12
19        IAID: 00000001
20

```

```

21         T1: 0
22         T2: 0
23
24 Frame 40948: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface lo, id 0
25 Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
26 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
27 User Datagram Protocol, Src Port: 547, Dst Port: 546
28 DHCPv6
29     Message type: Advertise (2)
30     Transaction ID: 0x171802
31     Client Identifier
32         Option: Client Identifier (1)
33         Length: 14
34         DUID: 0001000100000000eee60eb6c837
35         DUID Type: link-layer address plus time (1)
36         Hardware type: Ethernet (1)
37         DUID Time: Jan 1, 2000 00:00:00.000000000 UTC
38         Link-layer address: ee:e6:0e:b6:c8:37
39     Server Identifier
40         Option: Server Identifier (2)
41         Length: 14
42         DUID: 00010001300a4cd936a73db94eeb
43         DUID Type: link-layer address plus time (1)
44         Hardware type: Ethernet (1)
45         DUID Time: Jul 16, 2025 11:43:21.000000000 UTC
46         Link-layer address: 36:a7:3d:b9:4e:eb
47     Status code
48         Option: Status code (13)
49         Length: 24
50         Status Code: NoAddrAvail (2)

```

## 11. DHCPv6 Relay Agent Fails to Include Mandatory `Interface-Id` Option

## Markdown

```

1  rfc3315
2  20.1.1. Relaying a Message from a Client
3  If the relay agent cannot use the address in the link-address field to identify the
   interface through which the response to the client will be relayed, the relay agent
   MUST include an Interface-Id option (see Section 22.18) in the Relay-forward message.
4
5  rfc8415
6  19.1.1. Relaying a Message from a Client
7  If the relay agent cannot use the address in the link-address field to identify the
   interface through which the response to the client will be relayed, the relay agent

```

MUST include an Interface-Id option (see Section 21.18) in the Relay-forward message. According to RFC 3315/8415, if a relay agent cannot guarantee that the `link-address` it uses will be sufficient for the DHCPv6 server to determine the correct return path, it **MUST** include an `Interface-Id` option to provide an unambiguous identifier for the client's interface.

Our code audit of the `relay_upstream6` function (in `src/rfc3315.c`) reveals the following flaw:

1. The function unconditionally copies a configured local address (`relay->local.addr6`) into the `link-address` field of the `Relay-forward` message. Please see `rfc3315.c` line 2209.
2. Crucially, it **lacks any validation logic** to check if this `link-address` (which could be the unspecified address `::` or an address shared by multiple interfaces) is actually sufficient to uniquely identify the interface on which the client's message was received.
3. Then, the function **never adds the `OPTION6_INTERFACE_ID` option**, even in scenarios where it is mandatory.

Thus, we consider it may be a violation.

We do not have dynamic validation due to environment configuration.

### 13. Missing Validation for Mandatory Options in DHCPv6 Option Request Option (ORO) Processing

Markdown

```
1 rfc8415
2 21.7. Option Request Option
3 For certain message types, some option codes MUST be included in the Option Request option; see Table 4 for details.
```

Bash

```
1 root@5bfa19bcb2f8:~/projects/dnsmasq-2.91/src# echo "031616160001000e00010001000000
000011223344550002000e00010001300a4cd936a73db94eeb000800020000000300280000000100000
70800000a8c0005001899990db80badf00d00000000000123400000e1000001c20000600040017002
c" | xxd -r -p | nc -6u -q1 2001:db8
```

We specified `LQ_QUERY` in the Option Request of the Request message, but according to the provisions of Table 4, this is prohibited. Therefore, it can be determined that there is a lack of corresponding check logic in `dnsmasq`.

Markdown

1	+-----+-----+-----+-----+			
2		Option	Option Name ("OPTION"	Client ORO (1)   Singleton
3			prefix removed)	Option
4	+-----+-----+-----+-----+			
5		44	LQ_QUERY	No   Yes

Markdown

```
1 Frame 59557: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on inte
rface lo, id 0
2
```

```

Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
3 0:00:00:00:00:00)
4 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
5 User Datagram Protocol, Src Port: 52054, Dst Port: 547
6 DHCPv6
7     Message type: Request (3)
8     Transaction ID: 0x161616
9     Client Identifier
10         Option: Client Identifier (1)
11         Length: 14
12         DUID: 000100010000000000001122334455
13         DUID Type: link-layer address plus time (1)
14         Hardware type: Ethernet (1)
15         DUID Time: Jan  1, 2000 00:00:00.0000000000 UTC
16         Link-layer address: 00:11:22:33:44:55
17     Server Identifier
18         Option: Server Identifier (2)
19         Length: 14
20         DUID: 00010001300a4cd936a73db94eeb
21         DUID Type: link-layer address plus time (1)
22         Hardware type: Ethernet (1)
23         DUID Time: Jul 16, 2025 11:43:21.0000000000 UTC
24         Link-layer address: 36:a7:3d:b9:4e:eb
25     Elapsed time
26         Option: Elapsed time (8)
27         Length: 2
28         Elapsed time: 0ms
29     Identity Association for Non-temporary Address
30         Option: Identity Association for Non-temporary Address (3)
31         Length: 40
32         IAID: 00000001
33         T1: 1800
34         T2: 2700
35         IA Address
36             Option: IA Address (5)
37             Length: 24
38             IPv6 address: 9999:db8:bad:f00d::1234
39             Preferred lifetime: 3600
40             Valid lifetime: 7200
41     Option Request
42         Option: Option Request (6)
43         Length: 4
44         Requested Option code: DNS recursive name server (23)
45         Requested Option code: Leasequery Query (44)
46
Frame 59576: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on inte
47 rface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (0
48 0:00:00:00:00:00)
49 Internet Protocol Version 6, Src: 2001:db8::1, Dst: 2001:db8::1
50 User Datagram Protocol, Src Port: 547, Dst Port: 546
51 DHCPv6

```

```

52     Message type: Reply (7)
53     Transaction ID: 0x161616
54     Client Identifier
55         Option: Client Identifier (1)
56         Length: 14
57         DUID: 00010001000000000001122334455
58         DUID Type: link-layer address plus time (1)
59         Hardware type: Ethernet (1)
60         DUID Time: Jan  1, 2000 00:00:00.0000000000 UTC
61         Link-layer address: 00:11:22:33:44:55
62     Server Identifier
63         Option: Server Identifier (2)
64         Length: 14
65         DUID: 00010001300a4cd936a73db94eeb
66         DUID Type: link-layer address plus time (1)
67         Hardware type: Ethernet (1)
68         DUID Time: Jul 16, 2025 11:43:21.0000000000 UTC
69         Link-layer address: 36:a7:3d:b9:4e:eb
70     Identity Association for Non-temporary Address
71         Option: Identity Association for Non-temporary Address (3)
72         Length: 29
73         IAID: 00000001
74         T1: infinity
75         T2: infinity
76         Status code
77             Option: Status code (13)
78             Length: 13
79             Status Code: NotOnLink (4)
80             Status Message: not on link
81     Status code
82         Option: Status code (13)
83         Length: 24
84         Status Code: NoAddrAvail (2)
85         Status Message: no addresses available
86     DNS recursive name server
87         Option: DNS recursive name server (23)
88         Length: 16

```

## 12/14/15/16/17

We also noticed some mandatory rules related to the client side. Theoretically, dnsmasq, as the server, should have corresponding error message checking logic, but this might be controversial or lead to unnecessary mandatory checks. Therefore, we classify them under the last item as an optional fix.

The following has been verified: the server lacks the logic to check for violations of the corresponding messages.

Markdown

```
1  rfc8415
2  A DHCP client MUST include the INF_MAX_RT option code in any Option Request option
   (see Section 21.7) it sends in an Information-request message.
3
4  A DHCP client MUST request the Information Refresh Time option in the Option Reque
   st option (see Section 21.7) when sending Information-request messages.
5
6  A client MUST include an Elapsed Time option in messages to indicate how long the
   client has been trying to complete a DHCP message exchange.
7
8  A client MUST NOT request the Information Refresh Time option in the Option Reques
   t option in any other messages.
9
10 A client MUST include an Option Request option in a Solicit, Request, Renew, Rebin
    d, or Information-request message to inform the server about options the client wa
    nts the server to send to the client.
```