

# CVE-2018-15688 systemd dhcp6组件越界写漏洞分析

编译的话，用 `ubuntu 18.10`, 没有 `patch` 的源码下载路径

<https://code.load.github.com/poettering/systemd/zip/3941f8329a44596d77e9b9240f6e792656726fea>

漏洞位于 `dhcp6_option_append_ia`

```
switch (ia->type) {
    case SD_DHCP6_OPTION_IA_NA:
        len = DHCP6_OPTION_IA_NA_LEN;
        iaid_offset = offsetof(DHCP6IA, ia_na);
        break;

    case SD_DHCP6_OPTION_IA_TA:
        len = DHCP6_OPTION_IA_TA_LEN;
        iaid_offset = offsetof(DHCP6IA, ia_ta);
        break;

    default:
        return -EINVAL;
}

if (*buflen < len)
    return -ENOBUFS;

ia_hdr = *buf;
ia buflen = *buflen;

*buf += offsetof(DHCP6option, data);
*buflen -= offsetof(DHCP6option, data);

memcpy(*buf, (char*) ia + iaid_offset, len);

*buf += len;
*buflen -= len;
```

`buflen` 为 `buf` 剩余的空间大小，`len` 根据 `ia`这个选项的类型来确定

```

85     if ( v / )
86         return -22;
87     type = iaa->type;
88     if ( type == SD_DHCP6_OPTION_IA_NA )
89     {
90         len = 12;
91         iaid_offset = 2LL;           ←
92     }
93     else
94     {
95         if ( type != SD_DHCP6_OPTION_IA_TA )
96             return -22;
97         len = 4;
98         iaid_offset = 2LL;           ←
99     }
100    if ( *buflen < len )
101        return -105;
102    ia_hdr = *buf;
103    ia_buflen = *buflen;
104    *buf += 4;
105    *buflen -= 4LL;
106    memcpy(*buf, iaa + iaid_offset, len);
107    *buf += len;
108    *buflen -= len;
109    for ( addr = iaa->addresses; addr; addr = addr->addresses_next )
110    {
111        r = option_append_hdr(buf, buflen, 5u, 0x18uLL);
112        if ( r < 0 )

```

程序通过

```
if (*buflen < len)
```

来判断 buf 剩下的空间够不够存储 ia，但是后面通过 `*buf += offsetof(DHCP6option, data)` 相当于把 buf 的空间减少了 0x4 字节，这就有可能造成 4 字节的溢出。

**漏洞条件：**需要能劫持 dhcp 服务器，同时客户端要发送 dhcp6 的请求报文。

不过没有找到触发的方法，先贴一个发送 dhcp6 数据包的脚本。

```
from scapy.all import *
from time import sleep
```

```

sol = DHCP6_Solicit()
adv = DHCP6_Advertise()
opreq = DHCP6optOptReq()
et= DHCP6optElapsedTime()

duid = "00010001236be812000c292038db".decode("hex")
cid = DHCP6optClientId(duid=duid)
sid = DHCP6optServerId(duid=duid)
sid.add_payload("s"*800)

```

```
iana = DHCP6OptIA_NA(iaid=0xdeadbeef, ianaopts=DHCP6OptIAAddress(addr="fe80::431a:39d4:839d:215c"))

l2 = Ether(src="00:0c:29:27:59:f1")
l3 = IPv6(dst="fe80::431a:39d4:839d:215c", src="fe80::847:8219:1871:5a0f")
l4 = UDP()
pkt = l2/l3/l4/adv/iana/cid/sid

while True:
    sendp(pkt, iface='ens38')
    sleep(0.3)
```

## 参考

<https://bugs.launchpad.net/ubuntu/+source/systemd/+bug/1795921>

<https://github.com/poettering/systemd/commit/49653743f69658aeeebdb14faf1ab158f1f2cb20>

来源：<https://www.cnblogs.com/hac425/p/9882922.html>