CVE-2019-0547：DHCP客户端RCE漏洞

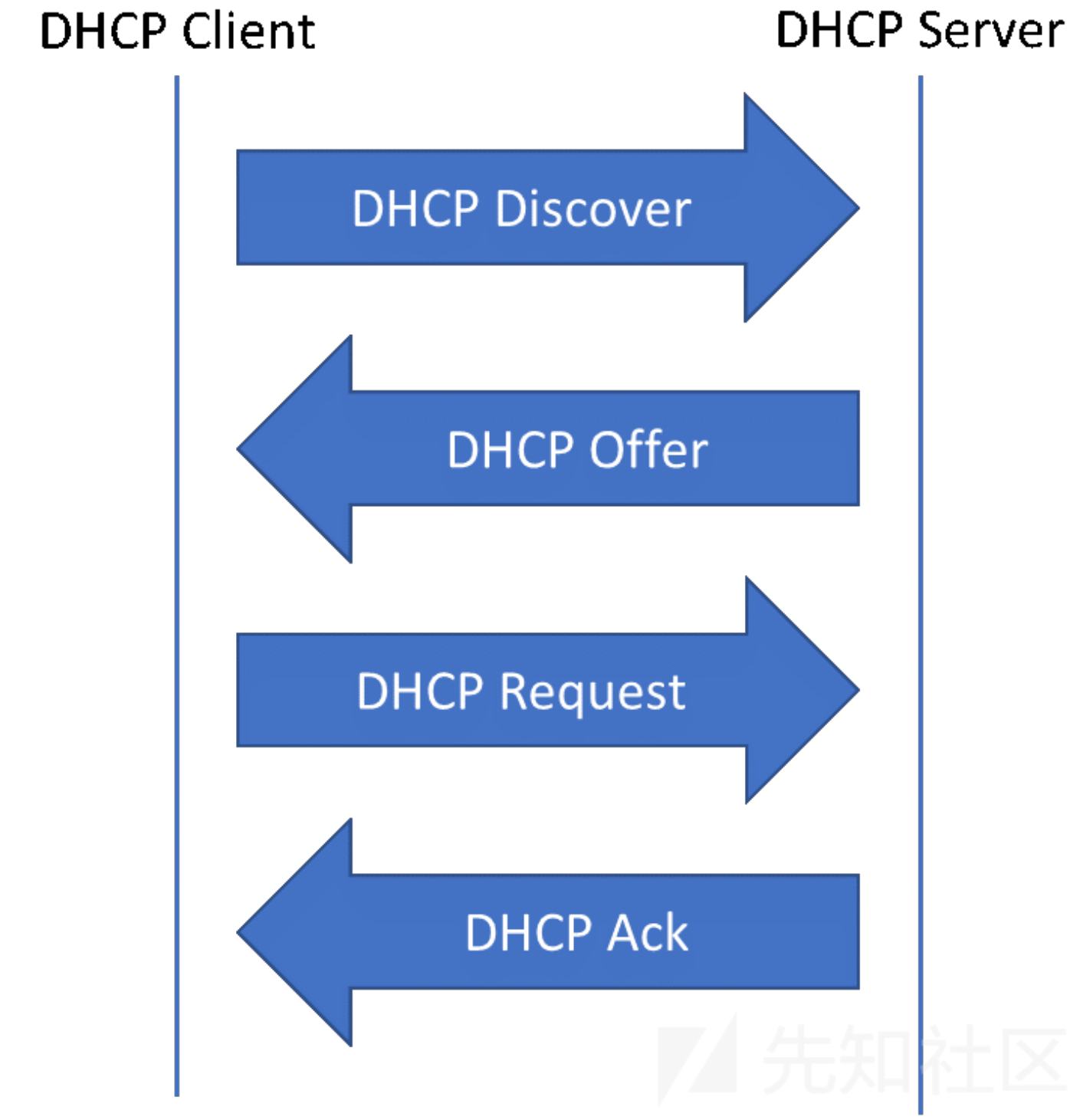
angel010 / 2019-08-08 06:29:00 / 浏览数 3951 安全技术 漏洞分析 顶(0) 踩(0)

CVE-2019-0547

CVE-2019-0547是今年微软修复的第一个漏洞，具体是系统中负责DHCP客户端服务的动态链接库dhcpcore.dll易受到DHCP reply包的攻击。
如果用户尝试连接到虚假DHCP服务器，攻击者就可以利用该漏洞来进行远程代码执行。

DHCP协议概述

DHCP是当计算机连接到网络时用来动态分配IP地址的C/S协议。DHCP服务器监听着67端口，并负责分配IP地址到DHCP客户端并分配TCP/IP配置到终端。
DHCP握手过程如下图所示：



在DHCP Offer和DHCP Ack之间，包中含有客户端加入网络所需的所有TCP/IP配置信息。DHCP ack包的结构如下所示：

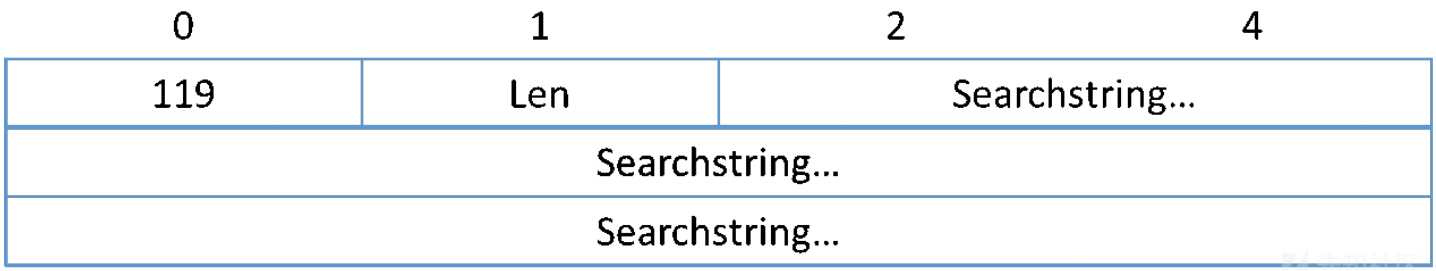
```
Dhcp: Reply, MsgType = ACK, TransactionID = 0x01903A3B
    OpCode: Reply, 2(0x02)
    Hardwaretype: Ethernet
    HardwareAddressLength: 6 (0x6)
    HopCount: 0 (0x0)
    TransactionID: 26229307 (0x1903A3B)
    Seconds: 3072 (0xC00)
    Flags: 0 (0x0)
    ClientIP: 0.0.0.0
    YourIP: 10.0.0.10
    ServerIP: 10.0.0.30
    RelayAgentIP: 0.0.0.0
    ClientHardwareAddress: E4-A7-A0-4E-BA-92
    ServerHostName:
    BootFileName:
    MagicCookie: 99.130.83.99
    MessageType: ACK - Type 53
    ServerIdentifier: 10.0.0.30 - Type 54
    IPAddressLeaseTime: Subnet Mask: 0 day(s),0 hour(s) 9 minute(s) 20 second(s) - Type 51
    SubnetMask: 255.255.255.0 - Type 1
    DomainSearch: DNS domain search list - Type 119
    End:
```

Options

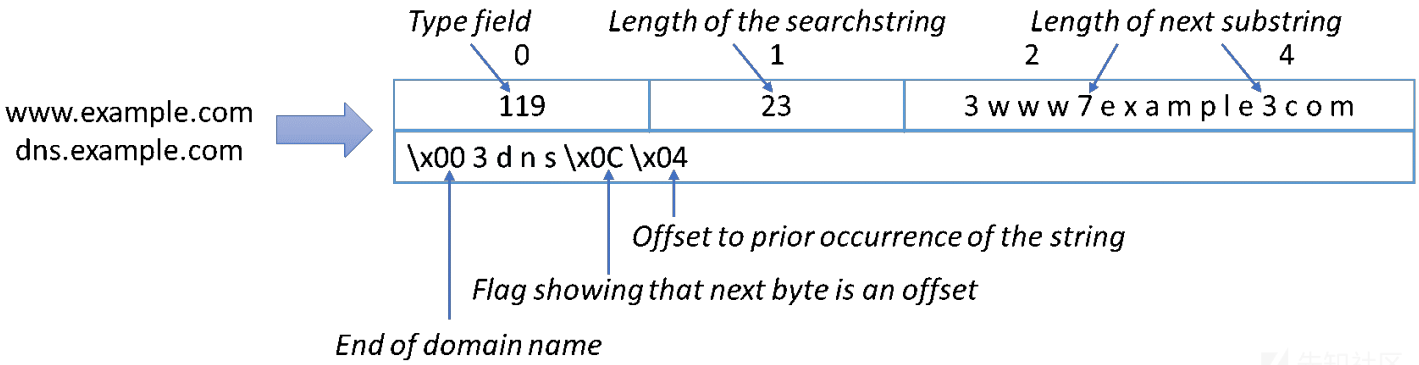
Options域有进行基本DHCP操作所需要的参数。其中一个是Domain Search (type field是119)。

Domain Search Option field (RFC 3397)

该option与OFFER和ACK包一起传递给客户端来指定使用DNS解析主机名时使用的域名搜索列表。DHCP option域的格式如下：

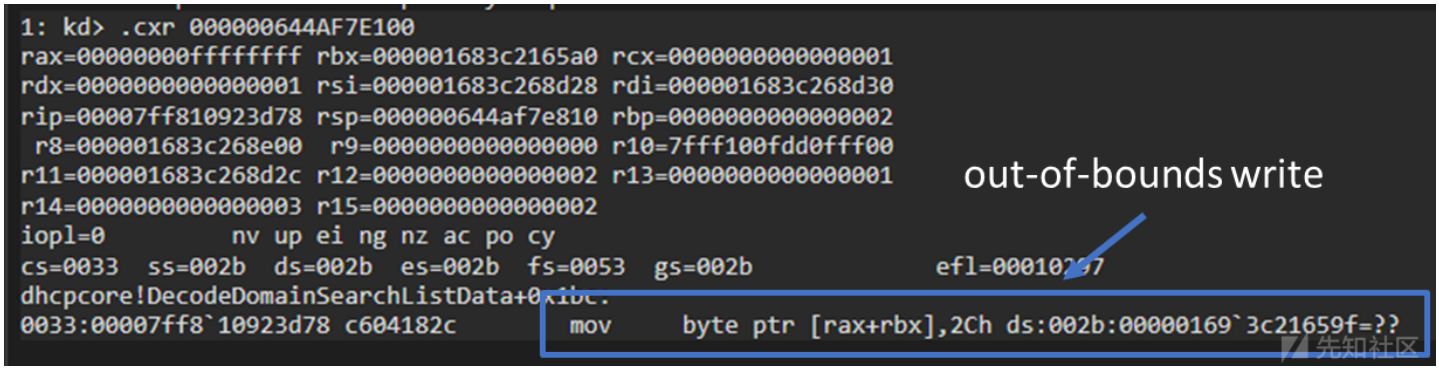


为了让searchlist编码紧凑一点，searchlist中的searchstrings是连接在一起编码的。www.example.com 和dns.example.com这样的域名都编码成了：



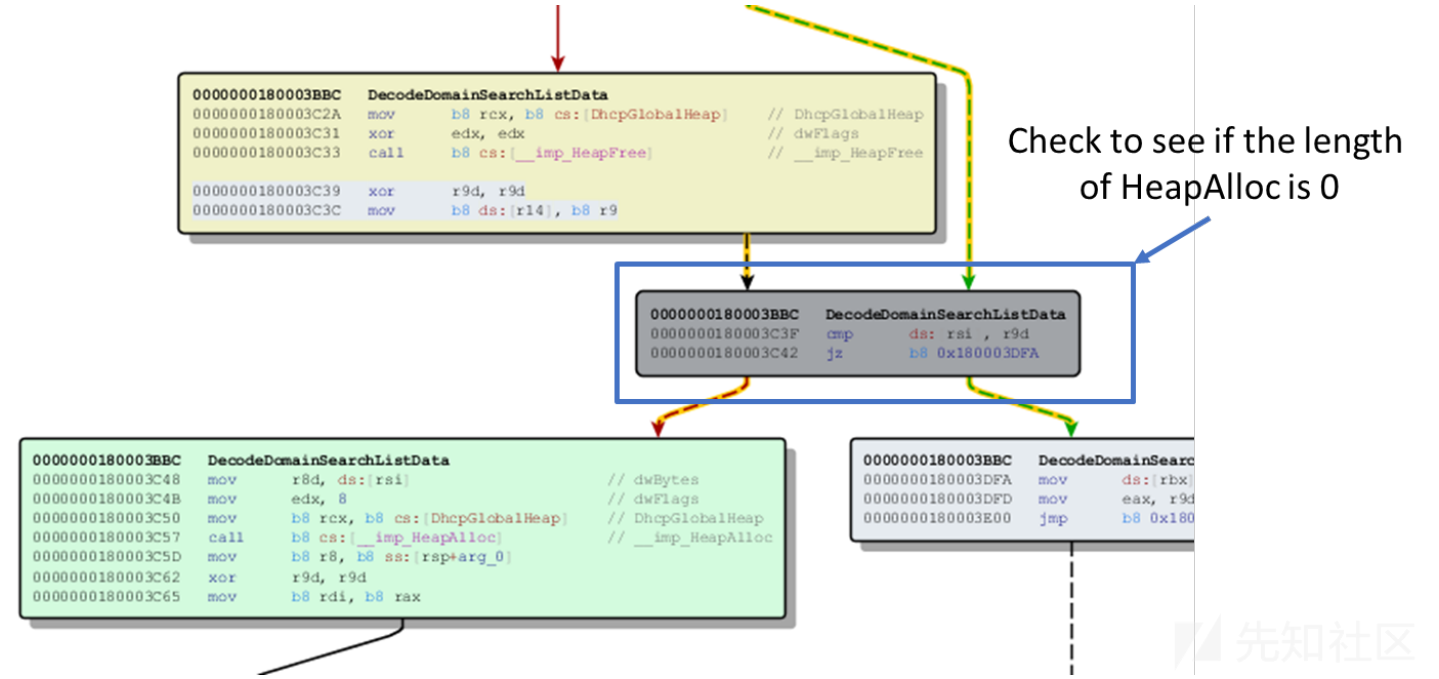
漏洞

而在dhcpcore.dll的DecodeDomainSearchListData函数中就存在着一个漏洞。DecodeDomainSearchListData函数解码了编码的search list option域中的值。在解码时，函数会计算解码的域名列表的长度，并分配内存并复制解码的列表。
恶意用户可以创建一个编码的search
list，比如当DecodeDomainSearchListData函数解码时，生成的长度为0。这会导致0内存的heapalloc，导致越界写。



补丁

补丁包含一个检查来确保到HeapAlloc的size参数不是0。如果是0，函数就会退出。



结论

网络中的恶意DHCP服务器可以通过回复来自客户端的DHCP请求来利用该漏洞。恶意DHCP服务器也可以说用户连接的无线AP。成功利用该来的可以触发客户端中的代码执

本文翻译自：https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/dhcp-client-remote-code-execution-vulnerability-demystified/