

## 0.1 CVE-2021-24086

According to Microsoft[4] CVE-2021-24086 is a denial of service vulnerability with a CVSS:3.0 score of 7.5 / 6.5, that is a base score metrics of 7.5 and a temporal score metrics of 6.5. The vulnerability affects all supported versions of Windows and Windows Server. According to an accompanied blog post published by Microsoft [6] at the same time as the patch was released, details that the vulnerable component is the Windows TCP/IP implementation, and that the vulnerability revolves around IPv6 fragmentation. The Security Update guide and the blog post also present a workaround that can be used to temporarily mitigate the vulnerability by disabling IPv6 fragmentation.

Figure out if this should be here

### 0.1.1 Public information

Due to the Microsoft Active Protections Program (MAPP)[5] security software providers are given early access to vulnerability information. This information often include Proof of Concept (PoC)s for vulnerabilities to be patched, in order to aid security software providers to create valid detections for exploitation of soon-to-be patched vulnerabilities. Due to MAPP, some security software providers publish relevant information regarding recently patched vulnerabilities. However, the information is usually very vague in details, and can therefore only aid in the initial exploration of the vulnerability. For CVE-2021-24086, both McAfee[9] and Palo Alto[8] posted public information about CVE-2021-24086. However, both articles contained very limited details, and is therefore far from sufficient to reproduce the vulnerability. Before trying to rediscover the vulnerability, the following information is available:

- The vulnerability lies within the handling of fragmented packets in IPv6
- The relevant code lies within the `tcpip.sys` drivers
- The root cause of the vulnerability is a NULL pointer dereference in `Ip_v6ReassembleDatagram` of `tcpip.sys`
- The reassembled packet should contain around 0xFFFF (65535) bytes of extension headers, which is usually not possible

### 0.1.2 Binary diffing

The usage of binary diffing to gather information about patched vulnerabilities is well described in current research[7][10], and has been made popular and easy to do by tools such as Bindiff[11] and Diaphora[3].

If we look at figure 1 we can compare the function changes of the patched and not-patched `tcpip.sys`. Looking at `tcpip!Ipv6pReassembleDatagram` we can see that the similarity factor is only 0.38 telling us that a significant amount of code has been changed.

write a little about how bindiffing works. Or don't idc.

## 0.1. CVE-2021-24086

---

| Similarity | Confid | Change  | EA Primary       | Name Primary            | EA Secondary     | Name Secondary          |
|------------|--------|---------|------------------|-------------------------|------------------|-------------------------|
| 0.16       | 0.27   | GI--E-- | 00000001C018D794 | sub_00000001C018D794    | 00000001C015A1D6 | sub_00000001C015A1D6    |
| 0.27       | 0.42   | GI--EL- | 00000001C01905B5 | sub_00000001C01905B5    | 00000001C01568FC | lppCleanupPathPrimitive |
| 0.31       | 0.73   | GI--E-- | 00000001C0190F38 | Ipv4pReassembleDatagram | 00000001C0190F68 | Ipv4pReassembleDatagram |
| 0.38       | 0.98   | GI--E-- | 00000001C0199FAC | Ipv6pReassembleDatagram | 00000001C019A0AC | Ipv6pReassembleDatagram |
| 0.42       | 0.62   | -I--E-- | 00000001C0154959 | sub_00000001C0154959    | 00000001C0001E42 | sub_00000001C0001E42    |
| 0.54       | 0.96   | GI----- | 00000001C019A658 | Ipv6pReceiveFragment    | 00000001C019A7F8 | Ipv6pReceiveFragment    |

Figure 1: Primary matched functions of `tcpip.sys`

Diving into the binary diff of `tcpip!Ipv6pReassembleDatagram` as seen on listing 1, we can clearly see a change. The first many changes from line *5-39* are simply register changes and other insignificant changes due to how the compiler works. However, on line *41-42* a new comparison is made to ensure that the value of the register `edx` is less than `0xFFFF`. This matches the statement given in subsection 0.1.1 (Public information), that the vulnerability is triggered by a package of around `0xFFFF` bytes.

```
1  --- "a/.\\unpatched tcpip.sys"
2  +++ "b/.\\patched tcpip.sys"
3  @@ -1,6 +1,4 @@
4  -sub     rsp, 58h          ; Integer Subtraction
5  +sub     rsp, 60h          ; Integer Subtraction
6  movzx   r9d, word ptr [rdx+88h] ; Move with Zero-Extend
7  mov     rdi, rdx
8  mov     edx, [rdx+8Ch]
9  -mov     bl, r8b
10 +mov     r13b, r8b
11 add     edx, r9d          ; Add
12 -mov     byte ptr [rsp+98h+var_70], 0
13 -and     [rsp+98h+var_78], 0 ; Logical AND
14 mov     [rsp+98h+length], edx
15 lea     eax, [rdx+28h]    ; Load Effective Address
16 -mov     rdx, rdi
17 mov     [rsp+98h+var_68], eax
18 lea     eax, [r9+28h]     ; Load Effective Address
19 mov     [rsp+98h+BytesNeeded], eax
20 -xor     r9d, r9d         ; Logical Exclusive OR
21 mov     rax, [rcx+0D0h]
22 -lea     rcx, IppReassemblyNetBufferListsComplete ; Load
    ↪ Effective Address
23 -mov     r13, [rax+8]
24 -mov     rax, [r13+0]
25 +mov     r12, [rax+8]
26 +mov     rax, [r12]
27 mov     r15, [rax+28h]
28 mov     eax, gs:1A4h
29 mov     r8d, eax
30 -mov     rax, [r13+388h]
31 +mov     rax, [r12+388h]
32 lea     rbp, [r8+r8*2]    ; Load Effective Address
33 -mov     r12, [rax+r8*8]
34 -xor     r8d, r8d         ; Logical Exclusive OR
35 +mov     rcx, [rax+r8*8]
36 shl     rbp, 6           ; Shift Logical Left
37 -add     rbp, [r15+4728h] ; Add
38 +add     rbp, [r15+4728h] ; Add
39 +mov     [rsp+98h+var_58], rcx
40 +cmp     edx, 0FFFFFFh    ; Compare Two Operands
41 +jbe     short loc_1C019A186 ; Jump if Below or Equal (CF=1 |
    ↪ ZF=1)
```

Listing 1: Diff of patched and vulnerable Ipv6pReassembleDatagram

Looking at the raw assembly without any knowledge of what the registers contain or what parameters are passed to the function can be very confusing. To make it easier for the reader to follow, listing 2 contains the annotated decompiled code of the vulnerable and patched `tcpip!Ipv6pReassembleDatagram` function. Here the patch is easy to spot, as the call to `tcpip!NetioAllocateAndReferenceNetBufferAndNetBufferList` is replaced with the check that we also observed in listing 1. The check is there to ensure that the total packet size is less than `0xFFFF`, which is the largest 16 bit value. The packet size is calculated on line 4-6 using the fragmentable and unfragmentable parts of the reassembled packet.

```
1  --- "a/.\\unpatched tcpip.sys"
2  +++ "b/.\\patched tcpip.sys"
3  void __fastcall Ipv6pReassembleDatagram(__int64 a1,
4  ↪ struct_datagram *datagram, char a3) {
5  unfragmentableHeaderLength =
6  ↪ datagram->unfragmentableHeaderLength;
7  packetSize = unfragmentableHeaderLength +
8  ↪ datagram->fragmentableLength;
9  BytesNeeded = unfragmentableHeaderLength + 40;
10 v6 = *(_QWORD *)(*(_QWORD *) (a1 + 208) + 8i64);
11 v7 = *(_QWORD *)(*(_QWORD *) v6 + 40i64);
12 LockArray_high = HIDWORD(KeGetPcr()[1].LockArray);
13 -v11 = NetioAllocateAndReferenceNetBufferAndNetBufferList(IppRea_
14 ↪ ssemblyNetBufferListsComplete, datagram, 0i64, 0i64, 0,
15 ↪ 0);
16 +if ( packetSize > 0xFFFF )
```

Listing 2: Diff of patched and vulnerable `Ipv6pReassembleDatagram`

At this stage of the vulnerability rediscovery process, the following requirements are now available:

- We have to abuse IPv6 fragmentation in `tcpip!Ipv6pReassembleDatagram`
- We have to construct a single packet with around `0xFFFF` bytes of extension headers
- We have to trigger a null dereference somewhere in `tcpip!Ipv6pReassembleDatagram`

The next section will give a primer into how IPv6 fragmentation works to better understand how we can fulfill the above-mentioned requirements.

### 0.1.3 IPv6 fragmentation primer

#### IPv6 Extension headers

[2, sec. 4.5]

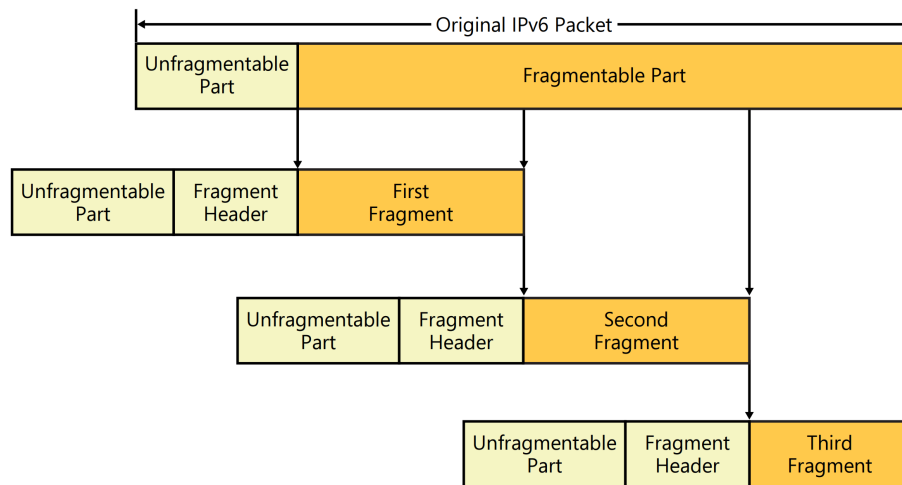
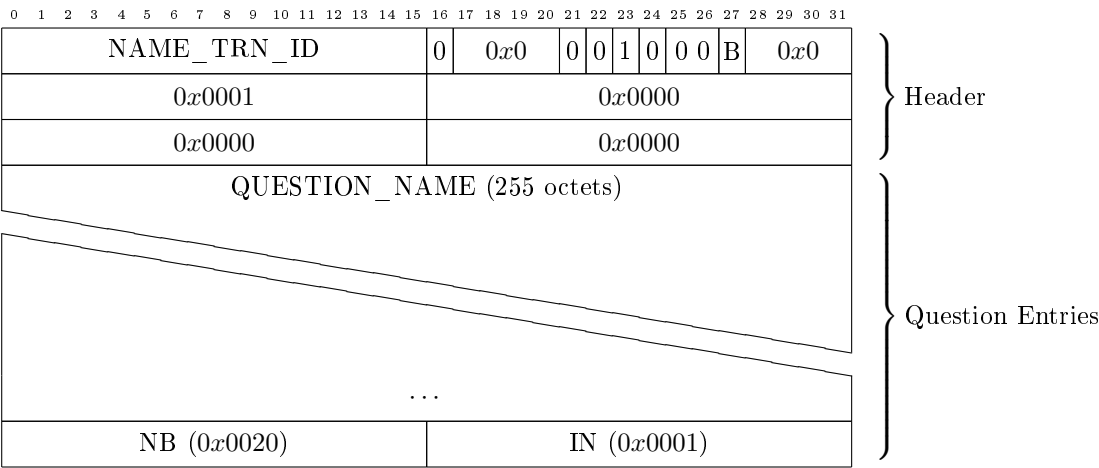


Figure 2: IPv6 fragmentation[1]



Where

**NAME\_TRN\_ID** is the transaction ID for the Name Service Transaction

**QUESTION\_NAME** is the compressed name of the NetBIOS name for the request.

Figure 3: IPv6 Fragment Header [2, sec. 4.5]

**IPv6 Fragment header**

**0.1.4 Root-cause analysis**

**0.1.5 Triggering the vulnerability**