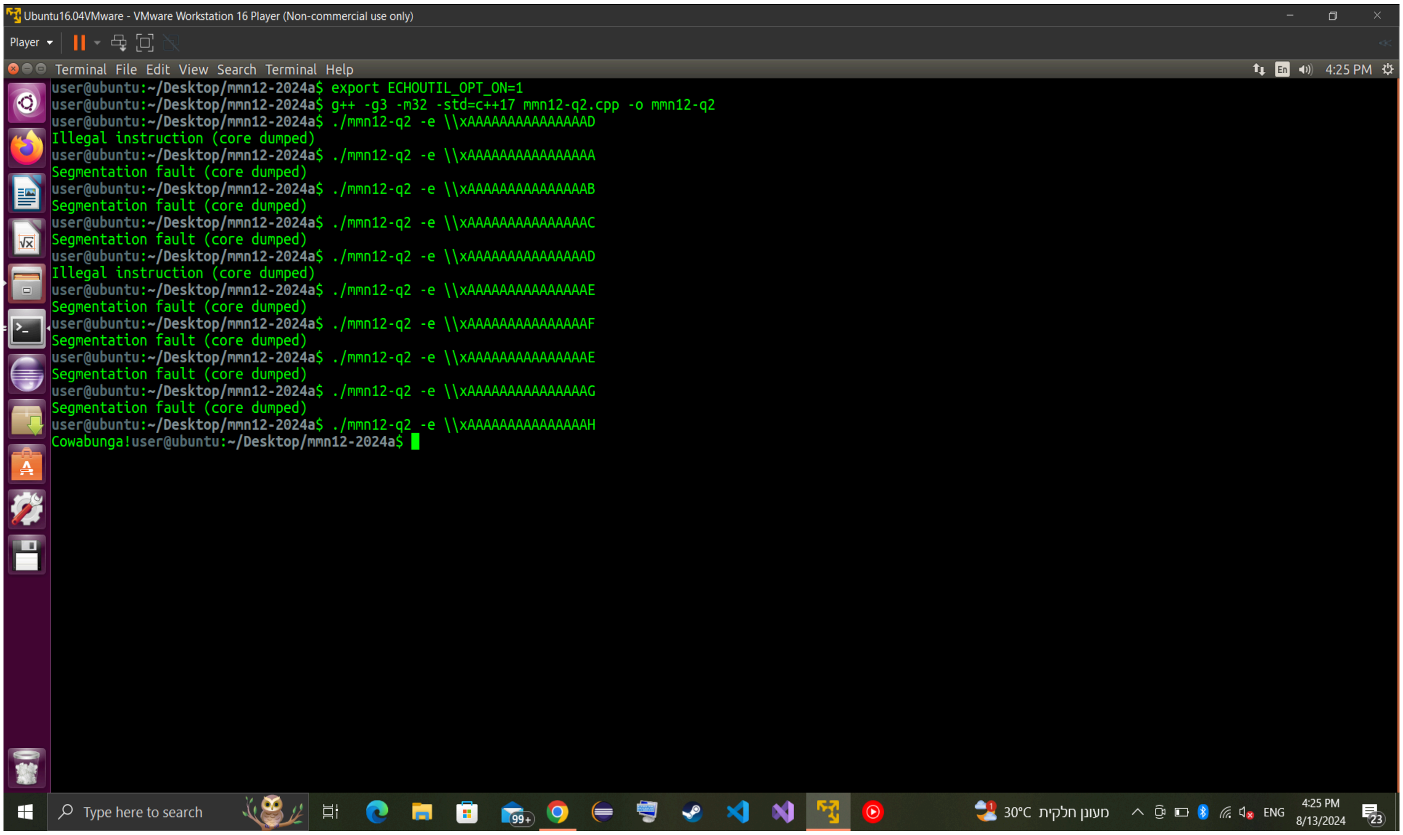
Threat	Calling function unreachable() that’s never called in the code, because of buffer overflow that input of user from the command line causes.
Affected component	To the program echoutil that a non wanted user can know the password now.
Module details	Mmn02-q2.cpp, void handle_escape(const char*);
Vulnerability class	Access-Control
Description	When created an environment variable named ECHOUTIL_OPT_ON (as I created in linux with export ECHOUTIL_OPT_ON=1), and the program is run with the arguments (in my computer): -e \\xAAAAAAAAAAAAAAAH The program calls the function unreachable() and prints the secret password ‘Cowabunga!’. This breach happens because of the fact that the program assumes that the user will put an argument with 16 characters at most, all arguments that starts with ‘\\’ character causes the program to enter the function handle_escape.we entered 17 characters after the ‘\\’ character, because of the fact that program does not check the length of the input from the user it takes all of those 17 characters into the l.buffer, and that causes an invasion of the next field of the struct-Handler that has a pointer to the VTABLE. In the situation above the last surplus character changes the pointer mentioned above. The character makes the pointer go back 4 bytes from its original position that's checked the last time the program runned. And when happens a call to the function helper(), that its address is vtable + 4, the program actually calls unreachable() that is in the address: *(VTABLE + 4 + -4) = *VTABLE, because of the offset, In the call to the function interpret, helper calls to unreachable that it’s address is in the pointer mentioned above because of the changes.
Result	Exposure of a hidden info of the application and its printing.
Prerequisites	Access to the run file of the program and to environment variables.
Business impact	A malicious third party can gain the secret password, and it can use that password for its purposes.
Proposed remediation	Checkup of the length of user input when the copy to the l.buffer happens and that it would not take more than 16 characters from that input.


Ubuntu16.04VMware - VMware Workstation 16 Player (Non-commercial use only)
Player
Terminal File Edit View Search Terminal Help
4:25 PM
Type here to search
30°C מעונן חלקית
ENG
4:25 PM
8/13/2024

```
user@ubuntu:~/Desktop/mmn12-2024a$ export ECHOUTIL_OPT_ON=1
user@ubuntu:~/Desktop/mmn12-2024a$ g++ -g3 -m32 -std=c++17 mmn12-q2.cpp -o mmn12-q2
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAD
Illegal instruction (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAA
Segmentation fault (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAB
Segmentation fault (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAC
Segmentation fault (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAD
Illegal instruction (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAE
Segmentation fault (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAF
Segmentation fault (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAE
Segmentation fault (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAG
Segmentation fault (core dumped)
user@ubuntu:~/Desktop/mmn12-2024a$ ./mmn12-q2 -e \\xAAAAAAAAAAAAAAAH
Cowabunga!user@ubuntu:~/Desktop/mmn12-2024a$ 
```