S32tan@uwaterloo.ca

Shjonathan Tan

21112183

In pwgen.c there is a format string vulnerability parse_args function and inside (case e) where there is a fprintf(stderr, buffer);

We are able to input a format string vulnerability here due to the argv[0] we are able to find the stack address.

The sploit1.c sets the value at 0x41 to Buffer size and the number of bytes starts from the buffer pointer. F_string writes to the address 0x4141ffbf 0x4141d950 %58n writes to the address, 54674 is a num that specifies the width of the field. This code is supposed to overwrite the Return address