THE UNIVERSITY of NEW ORLEANS

CSCI 4621/5621 Intro to CyberSecurity

06: Format String Exploits in C

Vassil Roussev

vassil@cs.uno.edu

Format functions

- printf Output a formatted string (FS)
- fprint Write FS to a file
- sprintf Write FS into a string
- snprintf Write FS into a string checking the length
- vprintf Prints the va_arg structure to stdout
- vfprintf Prints the a va_arg structure to a file
- vsprintf Prints the va_arg to a string
- vsnprintf Prints the va_arg to a string checking the length

Format parameters of interest

- %p
  - *output pointer → 0xFA4576A3*
- %x
  - *output hexadecimal → FA4576A3*
- %s
  - *print string at address*
- %<num>$<fmt>
  - *%11$p → 11th parameter as pointer*
- %n
  - ***output** number of characters printed*
- others
  - *%d, %c, %f, …*

Arbitrary read/write

- Vulnerable invocation
  - `printf(<input_string>)`
- Allows attacker to
  - *walk the stack*
  - *modify the stack*
  - *read arbitrary memory locations*
  - *write arbitrary memory locations*
- See
  - *fmt/fmt.c*