

More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format string PLT Trampo optimisatio demo

thanks

More Adventures In Format Strings

deanx

Portcullis Computer Security Limited



outline

More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash format strings PLT Trampoline

optimisation

demo

thanks

1 what?

2 pownage

- heap smash comparison
- luxuries of the format string
- PLT Trampoline



4 demo



what?

More Adventures In Format Strings

deanx

outline

what?

heap smash format strings PLT Trampol optimisation

 $What_{(not)}?$



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash format strings PLT Trampolin

·

uemo

thanks

Do some funky stuff (DL Style) and call free



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash format strings PLT Trampolir

optimisatioi

demo

- Do some funky stuff (DL Style) and call free
- Free overwrites 4 bytes



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash format string

PLI Trampoli

optimisatior

demo

thanks

Do some funky stuff (DL Style) and call free

- Free overwrites 4 bytes
- Where?



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash format strings PLT Trampolin

optimisatio

demo

thanks

Do some funky stuff (DL Style) and call free

- Free overwrites 4 bytes
- Where?
 - PLT



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash format strings PLT Trampoli

demo

- Do some funky stuff (DL Style) and call free
- Free overwrites 4 bytes
- Where?
 - PLT
- Why?



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash

format strings PLT Trampoline

optimisation

demo

- Do some funky stuff (DL Style) and call free
- Free overwrites 4 bytes
- Where?
 - PLT
- Why?
 - It's rw
 - It's static
 - It will get called again



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash format strings PLT Trampolin

optimisatior

demo

- Do some funky stuff (DL Style) and call free
- Free overwrites 4 bytes
- Where?
 - PLT
- Why?
 - It's rw
 - It's static
 - It will get called again
- What?



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash

PLT Trampoline

optimisation

demo

- Do some funky stuff (DL Style) and call free
- Free overwrites 4 bytes
- Where?
 - PLT
- Why?
 - It's rw
 - It's static
 - It will get called again
- What?
 - Pointer to trampoline that JMP's *edi
 - Where *edi contains your shellcode



More Adventures In Format Strings

deanx

outline

what?

pownage

heap smash format strings

PLT Trampoline

optimisatior

demo

- Do some funky stuff (DL Style) and call free
- Free overwrites 4 bytes
- Where?
 - PLT
- Why?
 - It's rw
 - It's static
 - It will get called again
- What?
 - Pointer to trampoline that JMP's *edi
 - Where *edi contains your shellcode
- Problem: What if you have no appropriate registers?



More Adventures In Format Strings

deanx

outline

what?

pownage

- heap smash format strings PLT Trampolin
- optimisation

demo

- Do some funky stuff (DL Style) and call free
- Free overwrites 4 bytes
- Where?
 - PLT
- Why?
 - It's rw
 - It's static
 - It will get called again
- What?
 - Pointer to trampoline that JMP's *edi
 - Where *edi contains your shellcode
- Problem: What if you have no appropriate registers?
- Solution: ?



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampolin optimisation demo

Arbitrary Memory Overwrite



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampolin optimisation demo thanks

- Arbitrary Memory Overwrite
- Non-contiguous Overwrite



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampolii optimisation demo

- Arbitrary Memory Overwrite
- Non-contiguous Overwrite
- Exploit: Follow Heap Smash Just Path



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampolin optimisation Arbitrary Memory Overwrite

Non-contiguous Overwrite

- Exploit: Follow Heap Smash Just Path
- Problem: What if you have no appropriate registers?



More Adventures In Format Strings

deanx

- outline
- what?
- pownage heap smash format strings PLT Trampolin optimisation demo

- Arbitrary Memory Overwrite
- Non-contiguous Overwrite
- Exploit: Follow Heap Smash Just Path
- Problem: What if you have no appropriate registers?
 - Again Jmp *edi will fail



More Adventures In Format Strings

deanx

- outline
- what?
- pownage heap smash format strings PLT Trampolin optimisation demo
- aemo
- thanks

- Arbitrary Memory Overwrite
- Non-contiguous Overwrite
- Exploit: Follow Heap Smash Just Path
- Problem: What if you have no appropriate registers?
 - Again Jmp *edi will fail
- Solution: Rewrite a register



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampoline optimisation

Use the format string



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampoline optimisation

demo

- Use the format string
- Write a small shellcode to the PLT



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampoline

demo

thanks

Use the format string

Write a small shellcode to the PLT

lea edi,[edi-2150]

jmp *edi



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampoline

optimisation

demo

- Use the format string
- Write a small shellcode to the PLT
 - lea edi,[edi-2150]
 - jmp *edi
- Point a PLT Entry to your chain code



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampoline

optimisation

demo

thanks

Use the format string

Write a small shellcode to the PLT

lea edi,[edi-2150]

- jmp *edi
- Point a PLT Entry to your chain code
- Now when it runs *edi will contain your long, stage 2 shellcode



More Adventures In Format Strings

deanx

outline

what?

- pownage heap smash format strings PLT Trampoline
- optimisation
- demo
- thanks

- Use the format string
- Write a small shellcode to the PLT
 - lea edi,[edi-2150]
 - jmp *edi
- Point a PLT Entry to your chain code
- Now when it runs *edi will contain your long, stage 2 shellcode
- Job Done



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampoli

optimisation

demo

thanks

• Why Optimise?



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampolir

optimisation

demo

thanks

• Why Optimise?

- Format Strings Are inefficient
- ~ 10 bytes in 2 bytes out (buffer space)
- Large Logs



More Adventures In Format Strings

deanx

Why Optimise?

- Format Strings Are inefficient
- \sim 10 bytes in 2 bytes out (buffer space)
- Large Logs
- What Can We Do?

- outime
- pownage heap smash format strings PLT Trampoli
- optimisation
- demo
- thanks



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampolin

optimisation

demo

thanks

• Why Optimise?

- Format Strings Are inefficient
- ~ 10 bytes in 2 bytes out (buffer space)
- Large Logs
- What Can We Do?
 - Write in any order
 - Write in the most efficient order
 - Write \x0a before \x1a before \x2a before \x3a



More Adventures In Format Strings

deanx

optimisation

Why Optimise?

- Format Strings Are inefficient
- \sim 10 bytes in 2 bytes out (buffer space)
- Large Logs
- What Can We Do?
 - Write in any order
 - Write in the most efficient order
 - Write x0a before x1a before x2a before x3a
 - 0x3a1a2a0a
 - 0x0a1a2a3a (1byte) or 0x2a0a3a1a (2 bytes)



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampolin

optimisation

demo

thanks

Why Optimise?

- Format Strings Are inefficient
- ~ 10 bytes in 2 bytes out (buffer space)
- Large Logs
- What Can We Do?
 - Write in any order
 - Write in the most efficient order
 - Write \x0a before \x1a before \x2a before \x3a
 - 0x3a1a2a0a
 - 0x0a1a2a3a (1byte) or 0x2a0a3a1a (2 bytes)

How?



More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format strings PLT Trampolin

optimisation

demo

thanks

Why Optimise?

- Format Strings Are inefficient
- ~ 10 bytes in 2 bytes out (buffer space)
- Large Logs
- What Can We Do?
 - Write in any order
 - Write in the most efficient order
 - Write x0a before x1a before x2a before x3a
 - 0x3a1a2a0a
 - 0x0a1a2a3a (1byte) or 0x2a0a3a1a (2 bytes)
- How?
 - Write Write Address in order
 - Use % the x'th memory location



demo

More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format string: PLT Trampol

optimisation

demo

thanks

demo!



thanks

More Adventures In Format Strings

deanx

outline

what?

pownage heap smash format string PLT Trampo

.

thanks

mu-b nico bambam doc