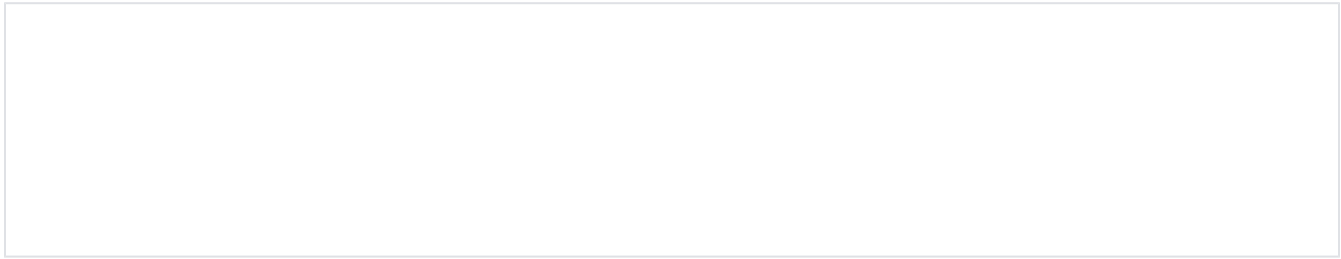


TechNote

Lazenc.a.0x0



Facebook Page

[Lazenc.a.0x0](#)

Page tree



Profile

- **Group**
 - [Twitter Profile](#)
 - [GitHub Profile](#)
 - [Facebook Profile](#)
- **Personal**
 - [Email](#)
 - [Linkedin](#)

Tool

Title	Creator	Modified
Pwndbg(scwuaptx)	Lazenc.a.0x0	Jul 27, 2018
PWNTTOOLS	Lazenc.a.0x0	Jul 20, 2018
Clang Static Analyzer	Lazenc.a.0x0	Nov 30, 2017
Valgrind - Memcheck	Lazenc.a.0x0	Nov 28, 2017
ASAN - Address Sanitizer	Lazenc.a.0x0	Nov 28, 2017
Ponce	Lazenc.a.0x0	Sep 25, 2017
Triton	Lazenc.a.0x0	Sep 25, 2017
angr	Lazenc.a.0x0	Sep 20, 2017
qira	Lazenc.a.0x0	Jun 29, 2017
pwndbg	Lazenc.a.0x0	Jun 29, 2017
PEDA	Lazenc.a.0x0	Jun 29, 2017

Heap exploits

Title	Creator	Modified
House of Orange	Lazenc.a.0x0	Apr 17, 2020
House of einherjar	Lazenc.a.0x0	Apr 17, 2020
The House of Lore	Lazenc.a.0x0	Apr 17, 2020
The House of Spirit	Lazenc.a.0x0	Apr 17, 2020
The House of Force	Lazenc.a.0x0	Apr 17, 2020
Unsafe unlink	Lazenc.a.0x0	Apr 17, 2020
Poison null byte	Lazenc.a.0x0	Apr 17, 2020
Overlapping chunks	Lazenc.a.0x0	Apr 17, 2020
unsorted bin attack	Lazenc.a.0x0	Apr 17, 2020
first-fit(Use-After-Free)	Lazenc.a.0x0	Apr 17, 2020
fastbin_dup_into_stack	Lazenc.a.0x0	Apr 17, 2020
fastbin_dup	Lazenc.a.0x0	Apr 17, 2020

Fuzzing		
Title	Creator	Modified
Wadi	Lazenc.a.0x0	Dec 13, 2017
libFuzzer	Lazenc.a.0x0	Dec 13, 2017
Honggfuzz	Lazenc.a.0x0	Dec 05, 2017
Boofuzz	Lazenc.a.0x0	Dec 04, 2017
Domato	Lazenc.a.0x0	Dec 04, 2017
AFL - American fuzzy lop	Lazenc.a.0x0	Nov 07, 2017
radamsa	Lazenc.a.0x0	Aug 20, 2017

Analysis		
Title	Creator	Modified
02.Dynamic program analysis	Lazenc.a.0x0	Nov 30, 2017
01.Static program analysis	Lazenc.a.0x0	Nov 30, 2017
Clang Static Analyzer	Lazenc.a.0x0	Nov 30, 2017
Valgrind - Memcheck	Lazenc.a.0x0	Nov 28, 2017
ASAN - Address Sanitizer	Lazenc.a.0x0	Nov 28, 2017
Valgrind	Lazenc.a.0x0	Nov 28, 2017
04.Concolic execution	Lazenc.a.0x0	Nov 28, 2017
06.DBI(Dynamic Binary Instrumentation)	Lazenc.a.0x0	Nov 28, 2017
05.Taint analysis	Lazenc.a.0x0	Nov 28, 2017
03.Symbolic execution(fe.at. Concrete execution)	Lazenc.a.0x0	Nov 28, 2017
DynamoRIO	Lazenc.a.0x0	Nov 17, 2017
Dyninst	Lazenc.a.0x0	Nov 17, 2017
PIN	Lazenc.a.0x0	Nov 17, 2017
IR(Intermediate Representation)	Lazenc.a.0x0	Sep 19, 2017

Basic exploit technical		
Title	Creator	Modified
02.Heap Exploitation	Lazenc.a.0x0	Oct 13, 2019
12.Heap Feng Shui	Lazenc.a.0x0	Apr 19, 2019
11.Heap Spray	Lazenc.a.0x0	Apr 18, 2019
10.One-gadgets(fe.at. PLT/GOT overwrite)	Lazenc.a.0x0	Apr 17, 2019
09.Race condition	Lazenc.a.0x0	Apr 16, 2019
08.BROP(Blind Return Oriented Programming)	Lazenc.a.0x0	Apr 15, 2019
04.Frame faking(Fake ebp)	Lazenc.a.0x0	Apr 08, 2019
02.Return to Shellcode	Lazenc.a.0x0	Apr 04, 2019
16.Stack pivot	Lazenc.a.0x0	Nov 07, 2018
15.Return-to-dl-resolve	Lazenc.a.0x0	Oct 02, 2018
14.Return-to-csu(__libc_csu_init)	Lazenc.a.0x0	Sep 06, 2018
13.JOP(Jump-Oriented Programming)	Lazenc.a.0x0	Aug 27, 2018
06.ROP(Return Oriented Programming)	Lazenc.a.0x0	Aug 15, 2018
07.SROP(Sigreturn-oriented programming)	Lazenc.a.0x0	May 27, 2018
05.Frame Pointer Overwrite	Lazenc.a.0x0	Apr 22, 2018
03.RTL(Return to libc)	Lazenc.a.0x0	Apr 11, 2018
01.Shellcode	Lazenc.a.0x0	Feb 23, 2018

Protection Tech

Title	Creator	Modified
06.PIE	Lazenc.a.0x0	Nov 28, 2018
05.PIC	Lazenc.a.0x0	Nov 28, 2018
01.NX Bit(MS : DEP)	Lazenc.a.0x0	Mar 18, 2018
04.RELRO	Lazenc.a.0x0	Sep 05, 2017
03.Canaries	Lazenc.a.0x0	Sep 05, 2017
02.ASLR	Lazenc.a.0x0	Sep 05, 2017

