TechNote

Lazenca.0x0

Profile

- Group
  - Twitter Profile
  - GitHub Profile
  - Facebook Profile
- Personal
  - Email
  - Linkedin

Tool

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

Fuzzing

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

Analysis

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

Heap exploits

Title	Creator	Modified
fastbin_dup_into_stack [English]	Lazenca.0x0	Jan 03, 2021
fastbin_dup[English]	Lazenca.0x0	Jan 03, 2021
Double free[English]	Lazenca.0x0	Jan 03, 2021
Double free[Korean]	Lazenca.0x0	Jan 03, 2021
House of Orange[English]	Lazenca.0x0	Jan 03, 2021
House of einherjar[English]	Lazenca.0x0	Jan 03, 2021
The House of Lore[English]	Lazenca.0x0	Jan 03, 2021
The House of Spirit[English]	Lazenca.0x0	Jan 03, 2021
The House of Force[English]	Lazenca.0x0	Jan 03, 2021
Unsafe unlink[English]	Lazenca.0x0	Jan 03, 2021
Poison null byte[English]	Lazenca.0x0	Jan 03, 2021
Overlapping chunks[English]	Lazenca.0x0	Jan 03, 2021
unsorted bin attack[English]	Lazenca.0x0	Jan 03, 2021
first-fit(Use-After-Free) [English]	Lazenca.0x0	Jan 03, 2021
House of Orange[Korean]	Lazenca.0x0	Jan 03, 2021
House of einherjar[Korean]	Lazenca.0x0	Jan 03, 2021
The House of Lore[Korean]	Lazenca.0x0	Jan 03, 2021
The House of Spirit[Korean]	Lazenca.0x0	Jan 03, 2021
The House of Force[Korean]	Lazenca.0x0	Jan 03, 2021
Unsafe unlink[Korean]	Lazenca.0x0	Jan 03, 2021

Find more results

Basic exploit technical

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

Protection Tech

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