VULNERABILITY DISCOVERY
Trainer: Dr. Silvio Cesare

Descripción general:

In this 2-day course, Vulnerability Discovery walks students through the numerous cases of undefined and platform specific behavior in C. We'll look at the C language, with numerous real-world examples of bugs found by the trainer. This course is focused on vulnerability research. Time will be spent on relating C memory corruption heap bugs to current attacks on the Linux Heap allocator. Moreover, we'll look for ways to automate bug discovery using fuzzing and static analysis.

Nivel del Training:

Avanzado

Temario:

Day 1 (Vulnerability Research)

Lectures:

- Virtual Memory
- Debugging
- Compiler Construction
- Data Structures
- Linux Heap Allocator Internals
- Fuzz Testing
- Dynamic Memory Checkers
- SMT Solving
- Symbolic Execution

Labs:

- ptmalloc Heap Metadata Corruption
- Fuzzing and AFL
- Dynamic Memory Checkers
- Static Program Analysis
- Coccinelle

Day 2 (C Bug Classes)

Lectures:

- Bugs in Preprocessor
- Bugs in Declarations and Initialisation
- Bugs in Expressions
- Bugs in Floating Point
- Bugs in Arrays
- Bugs in Characters and Strings
- Bugs in Memory Management
- Bugs in Input Output

Labs:

- Insecure Coding

Requerimientos:

Students taking Code Review should have an intermediate C Development background and hands-on experience with Linux. Hardware requirements for the class is an Internet connection as well as a laptop or workstation with a browser, SSH client and PDF viewer.

Reservá tu lugar

Costo:

USD 1.500

Reservá tu lugar

CONSULTAS

Para realizar consultas sobre el training o alguno de sus beneficios, escribir a: capacitacion@ekoparty.org

Trainer: Dr. Silvio Cesare

Dr Silvio Cesare is the Managing Director at InfoSect. He has worked in technical roles and been involved in computer security for over 20 years. This period includes time in Silicon Valley in the USA, France, and Australia. He has worked commercially in both defensive and offensive roles within engineering. He has reported hundreds of software bugs and vulnerabilities in Operating Systems kernels. He was previously the Director for Education and

Training at UNSW Canberra Cyber, ensuring quality content and delivery. In his early career, he was the scanner architect and a C developer at Qualys. He is also the co-founder of BSides Canberra - Australia's largest cyber security conference. He has a Ph.D. from Deakin University and has published within industry and academia, is a 4-time Black Hat speaker, gone through academic research commercialisation, and authored a book (Software Similarity and Classification, published by Springer).