Ali Raza

Lahore, 54590
Punjab, Pakistan
+92 305 7381431

Webiste: locus-x64.github.io
Email: elirazamumtaz@gmail.com

Research Interests

I am interested in identifying security vulnerabilities posed by Operating Systems and understanding their potential exploitation. As a Security Researcher at Ebryx, I specialize in Linux kernel exploitation and mainly focus on n-day research. I find Over-The-Air (OTA) exploitation interesting now, and I am exploring baseband firmware from an exploit developer's perspective.

Research Experience

nday ("Call of Death" in Shannon Baseband) - CVE-2020-25279
December, 2024 – Present
Ebryx (Pvt.) Ltd.

- Looking into Over-The-Air(OTA) communication in the mobile phone
- Explored different radio protocols used for mobile phone calls and SMS
- Looked into Samsung's Exynos modem chip that uses Shannon RTOS
- Used IDA Python and Ghidra scripts combined to load the firmware file for reversing
- Analysed the PAL memory allocation mechanism in Shannon
- Found the vulnerable code for the CVE mentioned above statically
- Working on FirmWire emulator to emulate the modem file and write RCE for it

0day in zlog (Famous C logging library) - CVE-2024-22857
November, 2023 – March, 2024
Ebryx (Pvt.) Ltd.

- Collaborator: Faran Abdullah
- Found Vulnerability in zlog using AFL++ providing arbitrary code execution
- Responsibaly disclosed the vulnerability to the maintainer
- CVE number - CVE-2024-22857
- Detailed blog post include Poc : www.ebryx.com/blogs

nday (Dirty Pipe) - CVE-2022-0847
April, 2023 – May, 2023
Ebryx (Pvt.) Ltd.

- Explored different data only attack in Linux kernel
- Looked into the in-memory buffer management inside kernel
- Following the source of pipe IPC in Linux kernel using elixir.bootlin, wrote a PoC for the CVE-2022-0847

Vulnerability Research and Exploit Development for Android Kernel, University FYP
July, 2022 – July, 2023
PUCIT - University of the Punjab

- Supervisor: Dr. Muhammad Arif Butt
- Worked on problems related to memory errors in binaries
- Worked on reversing binaries using IDA Freeware
- Worked on chroot jailbreak
- Worked on analyzing Linux kernel
- Worked on analysing msg_msg as exploit primitive
- Done with analysis of CVE-2019-2215 (nday)

Professional Experience

Malware Researcher March, 2023 – Present
Ebryx (Pvt.) Ltd. Lahore, Punjab, Pakistan

- Designed a kernel-level technique to detect path traversal attacks
- Working with a team looking for Linux user-land vulnerabilities and exploits and then introducing generic mitigation to cover that specific class of attack (e.g., Java Deserialization)
- Designed a kernel-level technique to patch ASLR brute forcing
- Found 0-day vulnerability as CVE-2024-22857 in a famous open-source library.
- Started looking for syzkaller to fuzz the Linux kernel.
- Working on Linux Kernel Exploitation (n-Day Research)
- Recognitions: Annual Best Performance Award 2023, Special recognition for the 0day

Teaching Assistant (Operating Systems) October, 2022 – February, 2023
PUCIT - University of the Punjab Lahore, Punjab, Pakistan

- Designed material and coursework for the newly introduced lab component of the subject
- Designed exam papers for the lab
- Assisted students in the lab + other TA responsibilities

Skills

Programming Languages: Assembly, C, C++, Python
Security: Binary Exploitation, Reverse Engineering, Vulnerability Research, Fuzzing, Exploit Development, n-day Research, OTA Exploitation
Tools: AFL++, syzkaller, IDA Pro, IDAPython, Ghidra, FirmWire, elixir by bootlin, GDB, GNU/Make
OS: Linux-x64

Education

PUCIT - University of the Punjab October, 2019 – July, 2023
Bachelor of Science - Computer Science Lahore, Punjab, Pakistan

- Graduated with CGPA 3.58/4.0
- Campus Lead of Google DSC
- President PUCon’23
- Member of the Cyber Security Society (Cyber@PU)

Punjab Group of Colleges, Okara Campus August, 2017 - September, 2019
Intermediate of Computer Science with Physics Okara, Punjab, Pakistan

- Graduated with 3rd position in BISE Sahiwal.

University Projects

Unix Shell C, Makefile
https://github.com/locus-x64/unix-shell

- An effort to write the *nix-based shell to gain an understanding of how the shell works and how OS creates and handles processes and allows processes to communicate with each other through its IPC interface

Exploits Scripts Python, x86 Assembly
https://github.com/locus-x64/exploit-development

- Basic scripts that I have written to solve some exploitation challenges

Hack Assembler C++

https://github.com/locus-x64/hack-assembler

- A 16-bit machine language assembler for the 16-bit Hack Assembly Language. It was done as part of building a complete 16-bit computer during the Computer Organization Assembly Language Course

Courses & MOOCs

Computer Systems Security: pwn.college

- Shellcode Injection
- Sandboxing
- Reverse Engineering
- Memory Errors
- Race Conditions
- Kernel Security
- Program Exploitation

Awards & Honors

Board Topper 2019

Intermediate - BISE Sahiwal Sahiwal, Pakistan

- (https://pgc.edu/our-achievers)
- Awarded with a brass medal and a cash prize by the Board of Intermediate and Secondary Education, Sahiwal