Gilbert Hoermann

www.seal9055.com | seal9055@gmail.com | https://github.com/seal9055 | linkedin.com/in/gilberthoerm

Experience

Interrupt Labs Vulnerability Researcher 07/01 - Current

- Performing vulnerability research focused on Chrome (V8 + Sandbox) and Android
- Manual code auditing/variant analysis and automated analysis using custom fuzzers and Codeql

Trail of Bits Vulnerability Research Internship 01/2023 - 02/2023

- Designed and implemented an efficient coverage guided graybox snapshot fuzzer on top of Qemu
- The fuzzer was able to leverage an Android live ram-dump to find bugs on an old device

UMass Cybersecurity Lecturer - *https://umasscybersec.org/cs390r.html* 01/2022 - 05/2023

- Teaching a course on reverse engineering and advanced vulnerability analysis to a class of 55 students
- Topics include re/code auditing, fuzzing, stack/heap exploitation, kernel-mode security, and automated dynamic/static software analysis w/ llvm, decompiler scripting, taint analysis, pin, and time-travel dbg

Technical Director at UMass Cybersecurity Club 11/2021 - 05/2023

- Hosting workshops focused on low level security topics such as binary exploitation and fuzzing
- Created virtualized enterprise network as training grounds for CPTC pentesting competition

Projects

Fuzzing Research using Emulation/JIT - *https://github.com/seal9055/sfuzz* 09/2021 - 07/2022

- Wrote an emulation-based greybox fuzzer focused on performance, code coverage and scaling
- The emulator + custom JIT enable high levels of target introspection without requiring source code
- The fuzzer includes coverage guided seed selection, byte level permission checks, snapshot fuzzing, memory allocation hooks and linear scaling across cores without a source requirement

Wyze Camera - *CVE-2021-43726 & CVE-2021-43727*

- Reverse engineered and emulated (using Qemu) device's firmware to find and exploit 2 critical bugs
- Rce via format string bug and remote image/video download by attackers via path traversal

Officejet Pro 6835 - *https://github.com/seal9055/officejet_pro_6835* *(In progress)*

- Project to find rce in popular printer. Currently extracting firmware through multiple layers of non-standard compression/encryptions that binwalk could not handle

Skills

- Reverse engineering, static analysis (binary ninja, llvm), and dynamic analysis (pin, gdb, triton, unicorn)
- Exploit dev, writing n-day (and ctf) exploits for userland, kernel (Linux), and browser (Chrome) bugs
- Bug discovery techniques, fuzzer harnessing, dataflow-analysis, patch diffing and variant analysis
- Understanding of modern exploit mitigations (ASLR, SMAP, HVCI, Sandboxing, ...) and bypass strategies
- Systems programming in the context of writing high-perf emulators, kernels, compilers and hypervisors
- Embedded VR, extracting firmware from flash, reversing decompression, emulation/fuzzing setup
- Ability to quickly tackle and get familiar with unfamiliar large codebases and binaries

Education

University of Massachusetts Amherst 08/2020 - 05/2023

- Graduated with BS in computer science with a focus on systems and security - GPA 3.8

Certifications & Achievements

OSCP - January 2021 **Sans Foundations** - June 2021

Ret2 Systems Binary Exploitation Course - *wargames.ret2.systems/course* 03/2021

Hypervisor Development for Security Researchers Course - *https://tandasat.github.io/* 08/2022

Ctftime Top 7 US - Binary exploitation player for k3rn3l4rmy