Zachary Cutlip

uid000 at icloud.com

Offensive Security Researcher

I like memory corruption, debuggers, and hex editors. I love a good, artisanal gadget chain. I like making tools that make all of those things easier. I love sharing what I've learned with others in person, in writing, or doing technical presentations.

Experience

Self Employed

Offensive Security Researcher, April 2023 - Present

- Conducted vulnerability research against iOS and macOS kernel and userspace
- Reverse engineered operating system components
    - To enumerate attack surface
    - Triage potentially exploitable bugs
- Identified high value, difficult to fuzz attack surface
    - Fuzzed binary-only targets including system libraries and daemons

Azimuth Security, LLC (now L3Harris Trenchant)

Offensive Security Researcher, May 2018 - March 2023

- Conducted vulnerability research against iOS and macOS kernel and userspace
- Extensively reverse engineered critical operating system components
- Developed tooling to aid vulnerability research and attack surface enumeration
    - Completely reverse engineered iOS binary sandbox format
    - Developed and maintained a binary-to-source sandbox profile decompiler

Apple, Inc.

Offensive Security Researcher, May 2014 - April 2018

- Analyzed numerous Apple technologies to catch vulnerabilities before shipping
- Audited kernel, security critical firmware, and userspace components
- Developed tooling and instrumentation to automate vulnerability discovery
- Committed code to shipping XNU to aid vulnerability research

Tactical Network Solutions, LLC

Senior Vulnerability Researcher, October 2011 - March 2014

- Conducted vulnerability research against embedded targets
- Developed surreptitious, post-exploitation capabilities
- R&D of exploitation techniques against new classes of targets
- Shared research via conference talks, whitepapers and technical blog posts

Raytheon Applied Signal Technology (formerly Seismic, LLC)

Tresys Technology, LLC

National Security Agency/USAF

Conference Presentations

- Infiltrate 2014
- 44CON 2013
- Black Hat USA 2012
- DEF CON 20

Projects & Publications:

- Practical Exploitation of Pegasus Kernel Vulnerabilities [1]
- Broken, Abandoned, and Forgotten Code: Parts 1-14 [2]
- Source Debugging the XNU Kernel [3]
- Reverse Engineering and Exploiting the BT HomeHub 3.0b [4]
- From SQL Injection to MIPS Overflows: Rooting SOHO Routers [5]
- Bowcaster Exploit Development Framework [6]

Education

- Johns Hopkins University: MS in Computer Science
- Texas A&M University: BBA in Information Operations Management

---

1. https://shadowfile.inode.link/blog/2022/07/revisiting-pegasus-on-ios9/ ↩

2. https://shadow-file.blogspot.com/2015/04/broken-abandoned-and-forgotten-code_22.html ↩
3. https://shadowfile.inode.link/blog/2018/10/source-level-debugging-the-xnu-kernel/ ↩
4. http://tinyurl.com/n9wnemp [pdf] ↩
5. http://tinyurl.com/agjr6bm [pdf] ↩
6. https://github.com/zcutlip/bowcaster ↩