

Michael N. Henry

Offensive Security Vulnerability Researcher

Chandler, AZ 85249
(503) 568-9612
root@michaelhenry.dev

EXPERIENCE

Facebook, Chandler AZ — *Offensive Security Pentest Engineer*

May 2020 - PRESENT

Finding vulnerabilities in third party products used by Facebook, Oculus, Whatsapp, and Instagram production environments. Directly responsible for finding massive scale vulnerabilities before attackers.

Intel, Chandler AZ — *Security Researcher*

May 2017 - May 2020

Found vulnerabilities in Intel products that impact millions of customers. Focused on Baseboard Management Controller firmware assessments, UEFI interactions with Management Engine, and Innovation Engine with roughly 30 CVEs and Intel-SAs assigned, and many more caught pre-release (no public disclosure).

Intel, Location — *Driver Development Engineer*

June 2011 - May 2017

Developed PCIe device drivers for various devices including Intel Xeon Phi coprocessors and Intel Omnipath network devices. Kernel mode experience in both Linux and Windows. Userspace tool and library development experience for various operating systems.

EDUCATION

Offensive Security Certified Professional (OSCP)

July 2017

Oregon Institute of Technology, Portland OR — BSc

June 2013

Bachelor of Science in Software Engineering Technology with a minor in Applied Mathematics.

SKILLS

Attacker mindset.

Finding 0-days.

Responsible Disclosure.

C/C++, Python, Go, C#, bash,
x86/x64 assembly.

Ghidra, Ida, fuzzing

CVEs

CVE-2020-8730

CVE-2020-8731

CVE-2020-8719

CVE-2020-8721

CVE-2020-8718

CVE-2020-8722

CVE-2020-8732

CVE-2020-8709

CVE-2020-8723

CVE-2020-8713

CVE-2020-8729

CVE-2020-8715

CVE-2020-8716

CVE-2020-8714

CVE-2020-8717

CVE-2020-8720

CVE-2020-0578

CVE-2020-0576

CVE-2020-0577

CVE-2019-11168

CVE-2019-0126

CVE-2019-0089

CVE-2019-0158

CVE-2018-3689

CVE-2017-5736

INTEL-SA-00036, 00039