Curriculum Vitae

Yeivin Nadav

Contact and personal information:

- Born in Israel 33 years of age.
- Currently Located at Petach tikva, israel.
- Current email address: sidt87@keemail.me.
- +972 (0) 521237440

Formal education and a selection of public work experience:

- 2015 – 2017: BSc Chemistry & Mathematics at the Hebrew University of Jerusalem.
- 2016 'Azure PCR' Software developer - Mainly QA, dealing with machine learning validation. (http://diagnostics.ai/)
- 2016 – 2019 Independent Security Researcher focuses on high end vulnerability research, fuzzing, Tooling, Exploit development, Reverse engineering and Mitigation Bypass.
- 2019 - 2020 Private consult Epica Tech LTD, Security Research (signed on NDA), i also managed a little team and was a totur to several Other employee's.
- 2020 & forward: General Computing research and consult: focuses on Hardware, Secure Computing, DFIR, "Root of Trust" Validation (SecureBoot-Apple,UEFI & BIOS Security, on- chip advanced programmable interrupt controller [AMD,INTEL]), Reverse engineering, Hardware Validation (OverClocking, Virtualization vulnerability research, Regulator Bypass and so on). I was able to find bugs with the SEPOS Validation for apple A11, i was able to expose both the INTC TPM, module the SPI HANDLER, and the ME, for intel IceLake, via a virtualization issue, for example i could expose the ME to a guest os and over voltage an i-3-1005G1 to a 20+ TDP UP..., i also Found issues with lenovo's firmware (for AMD), that could be used to circumvent The PSP. I Also dealt and focused on Networking, both client side and server, vpn's protocols and so on..

Notable achievements:

- **No 17 from Microsoft's Top 100 Hackers of 2018**. (https://blogs.technet.microsoft.com/msrc/2018/08/08/microsofts-top-100-security-researchers-black-hat-2018-edition/)

• **acknowledged by apple for disclosing security issues.** (https://support.apple.com/en-us/HT210355)

• **acknowledged by google for disclosing security issues** (https://bughunter.withgoogle.com/profile/fe386863-fdae-4164-bf31-b13d25d4b8e9).

• **ZDI SILVER status for 2019**. (https://www.zerodayinitiative.com/about/benefits/)

Selection of (used to be) Public writeup:

• CVE-2019-8658 - Pwning Webkit.

• MSRC-52108: Windows SBX and privesc via Race Conditions in the windows kernel.

• CVE-2019-8685: Safari bugs (https://github.com/ynad877/SafariTour)

• Messing around with the google fraud detection system.

• ZDI-18-428: Pwning MsEdge.

• ROP: Pwn the Windows Kernel with return oriented programming (https://github.com/ynad877/demos/blob/master/Win10/SmepByPassWin10x64build.16281Rs3/README.md).

• UAC Backdoors: about bypassing user account control on microsoft windows.

• kbMon: Writing A Ring O keylogger.

Selection of public vulnerability research:

(i should add that since I have found a lot more issues)

• (CVE-2019-8669) #2 Apple Safari, use of uninitialized stack variables leads to RCE.

• (CVE-2019-8669) #1 Apple Safari, Compiler logic error leads to RCE.

• (CVE-2019-8658) Apple Safari, improper binding between the compiler and the dom engine leads to UXSS.

• (MSRC-52108) Microsoft Windows, Race Condition with Win32k leads to EOP.

• (CVE-2019-8685) #1 Apple Safari, Compiler logic error leads to RCE.

• (issue 126413103) 'google.com', 'googleadservices.com' - fraud detection design issue.

• (CVE-2018-8251) Microsoft Windows, Media Foundation, UAF - RCE Vulnerability.

• (CVE-2018-8274) Microsoft Edge, UAF - RCE Vulnerability.

• (ZDI-18-577) Microsoft Edge, Type Confusion - RCE Vulnerability.

• (CVE-2018-8123) Microsoft Edge, UAF - Information Disclosure Vulnerability.

• (CVE-2018-1021) Microsoft Edge, OOB - Information Disclosure Vulnerability.

• (CVE-2018-0763) Microsoft Edge, Type Confusion - Information Disclosure Vulnerability.

• (CVE-2017-15303) CPUID CPU-Z Kernel Driver, OOB - LPE.

• (CVE-2017-15302) CPUID CPU-Z Kernel Driver, improper access permissions - LPE.

Introduction and a personal note:

I consider myself an autodidact in the field of computer science with a strong interest for Secure computing, program analysis and reverse engineering. I have worked with companies such as google microsoft etc and well-known contractors such as trend micro's ZeroDayInitiative as well as private contractors unveiling and exploiting security flaws in commonly used software. I possess a strong and vast knowledge in software security, that spans from logical errors to memory corruptions, from web technology to compilers and operating systems. I am comfortable with C/C++, Assembly (ARM, Intel x86, x64, Aarch64, desktop|mobile|embedded) and can code in many programming languages. I am comfortable with tools such as ida for closed source static analysis, or source code review for open-sources projects. I am experienced and comfortable with various debuggers and platforms. When needed I would develop my own tools in order to advance my research. During my work I have developed fuzzing tools and triaged countless memory corruption issues. I have reversed engineered closed source software from various windows applications to apple’s boot-loaders. I am adjudicated about software exploitation and have developed several exploits for 0-day flaws in software. Due to the nature of my work, a big percentage of my projects are closed sourced and NDA protected. I am well knowledgeable with a vast scope of different Security bug classes and have bypassed several novel-state of the art mitigation's. In addition I got knowledge about post exploitation and product design. I am aware of different web technologies, protocols, and wifi communications. I have experience with software development as well, from high level web servers to low level Computing (on multiple different architectures and platforms).

Such as: https://pastebin.com/kA3ik1kd,
https://raw.githubusercontent.com/ynad877/ipwndfu-8015/master/src/0x8015.S

Kind Regards: Nadav