Curriculum Vitae

Yeivin Nadav

Contact and personal information:

- Born in Israel 33 years of age.
- Currently Located at tel aviv, israel.
- Current email address: Ny87@protonmail.com.
- +972 (0) 541237440
- https://keyserver.ubuntu.com/pks/lookup?op=get&search=0x0e7ace675c73f0d4. (also inlined here)

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.
- 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 Securiy, 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 overvoltage an i-3-1005G1 to a 20+ TDP UP..., i also Foundd issues with lenovos firmware (for AMD), that could be used to cercumvent The PSP (i used S540-13Are, R7-4800u), to install a bios-level backdoor, from windows SecureBoot Operating system. I Also dealt and focus on Networking, both clientside and server, vpn's protocols and so on..

Notable achievements:

- No 17 from Microsoft's Top 100 Hackers of 2018.
- acknowledged by apple for disclosing security issues.
- acknowledged by google for disclosing security issues.
- ZDI SILVER status for 2019.

Selection of __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.
- Messing around with the google fraud detection system.
- ZDI-18-428: Pwning MsEdge.
- ROP: Pwn the Windows Kernel with return oriented programming.
- 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 issue's but they wer'e NeverReleased..)

- (CVE-2019-8669) #2 Apple Safari, use of uninitialised stack variable 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 bootloaders. 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 mitigations. 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/m1stadev/ipwndfu-8015/master/src/0x8015.S

Kind Regards: Nadav.

PKS:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Comment: Hostname:
Version: Hockeypuck ~unreleased

xsFNBGG2Hb0BEAC6l2G87eZbtzsJwcXlByQ2g8ThvJCnr1EXjy4FW4YeRJxWNh5w
lLntZaez4JofkLbM/34aNS3JypH2+Y7MLvecDntjVH2GyJRxfli+byGpjiqcJ56V
fbBF716IF79B6vHWu02MwcJN1p53YktF6kvZhOCgxv+NWXIlj4+ntz7DQHzZ1fJo
bOmyZgJk3bpoX4CjSm+kxwVzHcFfLcUrEin2SilUbFKLn/TN5fJbyeT2OZGGr5SX
dl3Rpf+nTFfGlDSkCEutoITAjKW5sE4BAz3lErs/i9epiZn7AYdt0cfk6hmdb9+2
RNkTMmdIfMKxBBy6JvPbuLxkYfyG2CVIjK2mEvEjAjpUbURdBZy18u/WJPe4t7bg
kPg2VABCr3doNCQRWvMTLM7JI2JxMruDATKKB2eDnh6KhWYpqooy0Df29zzLIIRy
DoQASqxFBSrI0EB31I9fb2a5cnBYpLrLiL1plaDBOwF5QMnQsYWejau4zN4AIsvl
JB3leftui0EwTkbLEBoMebrUgzmwOMnBpd+RIWLZ7IGVprELl0MtG9Xx1fgqIUif
HfJ91AlF5rwODYU3XhzYZ7NEIXZ0SEvJ3diTDnveYuAjtNpj6ICE14C8k/vkeD2X
2vhflZcyl2B56prjXPpi0o9QtMjG7K55qK//4yB0nlwTscpZEjQYrdFFdQARAQAB
zSlOeTg3QHByb3Rvbm1haWwuY29tIDxOeTg3QHByb3Rvbm1haWwuY29tPsLBjQQQ
AQgAIAUCYbYdvQYLCQcIAwIEFQgKAgQWAgEAAhkBAhsDAh4BACEJEA56zmdcc/DU
FiEEGtOasVuDVFMtd1YJDnrOZ1xz8NTGixAAp/R5OT86gNRMeZA68PQZ0v1SseBS
bLjz4nI186N1UeuWLMhl17Y8Z/Gfms8qTxi5Ns7KyQlmFYByYmwg7aYG7coqkozk
bw2SngoAIZexR/gLlGkI/liQ9Axygl9yDfXPzQzlKeXb1mBun2KrR8zUusw85AFo
4aUl2wvHNdDkjjT5y1KOVJi+yCP9jgFGx2To+1268MNYCdE9OTPCErnoMvcC3Irm
/+VC78L51/FeWvN5Uv5VK76fCfqmhDcnLh7fBAMysOcwyCLC8h3ZPGxAnCcId2oF
E9RhfNNgVsRQAq0irDFY0j1HTAFhj3UVD83KGXG/EsPlVpWJ8UDv2XhKaIw8TSRd
C15vgR3wdJMgmc53fwf3JJnxx1aOJN29EPgKF7u0dBqr+bvPFyRLfYx1Wjz8rJQm
dVBeBYRTZa29FT9QJ/60KVq2Egbfy1brGlLomLwB8+E2993wamgf6BxopzJ5DloF
p5HTTYMD6g4fHyBs0NmA8wrUaHu5OyNg3TNz414f12MeF92acmBobP4caiLc9WE+
qleS8ZBteImmDriAFra0yyLjo+Mr7mZetTnPZUaprOqMoMFnL2cA9QDe6t+UYoVw
gZnnJPZzhgb1OLP6tg6Qv0H0ZGjCePeee7l4zsCiXVntpCbeyCAdMujzPqvnYTLL
kLfcxdlc+8Y2nA3OwU0EYbYdvQEQANDxvD+Hz699rjc9YJ2Pzc4Ppvoak2ayNly7
BDk5qx6EPL/NbnV8T/XOpNLecD01zJxSirTT0XzKEsOuiFM2D/s5sRmWagwoNGSX
DQK5DIkWI7pR2ZnGC1mJy2vuYL+fb8r9vFmFaUBwufCWJisA4GpCQsoUBFjUj+ka
Ay1axy7bNijKfGYAhu537wfs8Zv0rAhYhhEZYhC7sBOCApI59IJod1ileN+4ieC5
LUOgWitSNr7g6/NkPeJwSMImYyRJVVnmo7oaptDdSr8ASqu2eQNUc4iUwImukJtT
vxlDgJt/K/v3UNtRkQ+cbrhS8/dfyx79/u7wIE4O5YDTc0K6vt7mR6B7c+qHiIpB
o76Rc2DA3sMHGcaxNnEvs71Ra84cZUN7mkXqoaz3Mh90auKleA2tTSzGDM/nH0Co
ptWLNfZ6gpkCEZ6HjrJcKfquE+o6hMgQvUdhf85mA6Oe/e0aUjAIjhwRXJQi1Ent
P0GSU2c0biQ6A4nuh0VSfAbEqgYdEKOoS7MKRC0T9Q9DjV4r/cibod4AJ4A46iUg
6i5DQ47oxBL+BGnj88jGITHWAiXpsuf26eTTKIaiVYghFFqzObdxBj8AY+OPU3aL
lss7omYbJgnBPLoQ8YAq7Uk0DOdRnLpxgXxHzsa+ktFsvd1eWrC+4w6BJ1euQRnN
TLoc7qmfABEBAAHCwXYEGAEIAAkFAmG2Hb0CGwwAIQkQDnrOZ1xz8NQWIQQa05qx
W4NUUy13VgkOes5nXHPw1EFVEACE54s6+nd9etjVzqoIIjSOIHCZfF08DevL4JdK
tgD50ZYjMR/J7tFY1Ffypxbo4sAxYxVBDwkbdsCzBrLBefIXCwwxpO1bhd5An/1r
mqSlPYA2pai3rZ5HHVkmrXxMCpPWYbiNVRsmLAJEjAsKdJJRfgS18PN06W67bUF4
IzV7L56QDyQg1/B4vGyGWSuiNqP/v6S9SZgjKHHh9C/k4N72H5CR/e1Rb9CHWjUm
+CnJhET/BT7wrQRKgm6fUr738LtE9King37ax7wXPIg05gsfOzIbtJqBiXg/fRAY
PAPjbokfqEH1CB/PT6fUhEepY6LLBpuy3Uh5W9GQQuJTRyiKc8qssLHn/RYlkNNY
56PimeZv9fUzIWT3ed+xm0Xpy78xlAUCu6tEVjfURO4SiPT91z6If2U/TU7Ndfgz
YYR7qEkyLfs5fsttb5Llxj5HEqu0nw3A7aa1LTgb2ocmXID0WvkM6LSY+7EnQbMY
4sq+de1C892UICZ7b0rzWmBDjwD8imTX6sYNMTzJ5Esdi4xISouMnsIAT/tcJtHp
n8zzSO8Nj1uAvoUf3rl0pYlN0PuWvGMKv612l7nZalF9r12X7Fd/0y1cu04stPvW
W9iPUgGq3gJPpLUEvvv7K9NAvJoUTtqPHgI4TwdTp/dh9jpch/nnSoZHOn4KxjQc
MrVGAw==
=0sHX
-----END PGP PUBLIC KEY BLOCK-----