Vishnu Dev T J

vishnudevtj.github.io | vishnudevtj@gmail.com

EDUCATION

Amrita Vishwa Vapeetham
Bachelor of Technology in Computer Science
Amrita School of Engineering
Amritapuri, India
July. 2017 – present
Current CGPA: 8.76/10

LINKS

Github:// vishnudevtj
Gitlab:// vishnudevtj
Twitter:// @vishnudevtj

ACTIVITIES

VULNERABILITY RESEARCH

- CVE-2019-14378 : Qemu [Link] [Exploit]
- CVE-2020-7039 : Qemu [Link]
- CVE-2020-7454 : FreeBSD [Link]
- CVE-2020-7455 : FreeBSD [Link]
- CVE-2020-2929 : VirtualBox [Link]

EXPLOIT DEVELOPMENT

- Wrote exploits for public bugs such as CVE-2017-11176
- Designed a course to introduce ARM exploitation [Link]
- Gave a talk on "Turning bugs into Exploits" which introduces different stages of exploit development [Slides]

TECHNICAL SKILLS

SKILLS

Binary Exploitation • Reverse Engineering • System Security • Fuzzing

LANGUAGES

Rust • C • Python • assembly(x86, ARM) • Bash • elisp

TOOLS

GDB • Ghidra • IDA Pro • Radare2 • Pwntools • Frida

PLATFORM

GNU/Linux • Microsoft Windows • Mac OS X

EXPERIENCE

TEAM bi0s MEMBER | CTF Team , Amrita Vishwa Vidyapeetham

2017–present | Amritapuri, IN

- Reverse Engineering and Binary Analysis of Linux/OS X binaries
- Linux Kernel/Userspace exploitation in x86 and ARM architecture
- Exploitation of heap based memory corruption bugs

InCTF | Core Organizing team and Challenge Author

2018–present | Amritapuri, IN

InCTF is India's leading CTF with acclaimed International, National and Junior editions.

- Developed Binary Exploitation challenges, which introduces different aspects of the area to the players
- Created infrastructure in docker to host Binary Exploitation challenges
- Visited schools to raise awareness about cyber security

PROJECTS

SNOWFLAKE | Debugging utility [Link]

Sep 2019 – Nov 2015

Rust based application which scans for patterns in the memory of a running process. It helps exploit developers to find pointers and offsets of data in the process.

Personal Research | Auditing Security of QEMU [Link]

Jun 2019 – Aug 2019

Audited the code of QEMU, and found a heap based buffer overflow bug in the network module. It was reported to Red Hat and CVE-2019-14378,CVE-2020-7039 was assigned. The bug was also weaponized to get VM escape.

HYPE | Toy Hypervisor [Link]

Mar 2019 – May 2019

Implemented a hypervisor which utilized the KVM API of Linux kernel, and executes 64 bit x86 assembly code to create better understanding of how modern hypervisors work.

DYNAMIC MEMORY ALLOCATOR

Jun 2018 – Aug 2018

Allocator written and implemented in C language and uses segregated freelists combined with the first fit and best fit selection algorithm.

ACHIEVEMENTS

Nov 2019	Winner of the Pwny Racing Episode 10 Live streamed head-to-head hacking competition
Oct 2019	Finalist for 5th XCTF International League as a part of Team bi0s CTF Conducted by Cyber Peace Technology, China
Sep 2019	Winner of the Write-up Competition Google CTF 2019
Sep 2019	Champions at HackLu on-site CTF 2018 as a part of Team bi0s CTF Conducted as a part of the Hack.Lu Cyber Security Conference
Mar 2019	Student Scholarship Awardee and Packet Wars Winner Troopers 19, Heidelberg, Germany