

M2 CySec 25-26

« Advanced Security »

Oral presentation

Option 1 : study of a CVE

■ Objective

- Understand – **and explain** – a (recent) published **exploitable** CVE
- (Try to) reproduce a **PoC** of the exploit
- Discuss the existing/appropriate **patch /mitigation** options

■ Expected output (by group of 2)

- A short **presentation + demo** (~ 20 minutes)
- A short summary (2 pages)

■ Schedule

- From now to **January the 5th**

Main issue: choose a CVE

- **Related to a security topic you are interested in:**
 - Application level (including web vulnerability)
 - OS level (Windows, Android, etc. are welcome!)
 - Network component, firmware, HW/SW interface, Etc.

- **Well enough documented/understandable**
 - Poc exploit and patch information available

- **« Easy » enough to reproduce ...**
 - Vulnerable code still available !
 - VM or Docker image of the exploit available?

How to proceed ?

■ Take the time to look for existing sources ...

NIST CVE database: <https://nvd.nist.gov/vuln/search>

Exploit database: <https://www.exploit-db.com/>

Some known exploitable vulns: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Google Zero RCA project: <https://googleprojectzero.github.io/0days-in-the-wild/rca.html>

Numerous available blogs (security companies, independent (ethical) hackers, etc.)

■ Set up the appropriate environment you need ...

- Docker (+ Dockerfile or docker image)
- VM
- Emulator?

■ Ask for help if necessary!

Option 2: Research paper presentation

▪ Objective

- Understand – and **explain** – a (recent) research result
- Chosen among a provided list of paper (or approved by the teaching staff)
- Numerous security-related topics available ...

▪ Expected output (by group of 2)

- An **oral presentation** (~ 20 minutes)
- A short summary (2 pages)

▪ Schedule

- From now to **January the 6th**

▪ Remark

- Re-using existing materials (slides, video, etc.) is allowed but:
 - Should be correctly credited ...
 - Video replay is forbidden!

How to proceed ?

■ Choose a topic you are interested in:

- Software vulnerability analysis and detection
- Web security
- Attack countermeasures
- Use of ML techniques for security
- Reverse engineering techniques and/or code (de)-obfuscation
- Security for mobile platforms (Android, iOS, etc.)
- Malware detection and analysis, etc.

■ Find a well-explained paper (and slide set)

- USENIX security conference papers are good candidates ...

■ Ask for help if necessary!