

The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

National Sun Yat-sen University

March 24, 2021
v1.0

Outline

- 1 Outcome
- 2 Related works
- 3 Current progress
- 4 Reference

Outcome

Outcome

No outcome.

Related works

Two papers

- A Measurement Study on Linux Container Security: Attacks and Countermeasures[1]
- Container-Based Cloud Platform for Mobile Computation Offloading[2]

Some Golang/Rust

- 1 The next generation of C/C++
- 2 High Concurrency, Memory Safe, Traits

ASLR/KASLR/Finer-grained KASLR

Capabilities

Table 3: Function of Security Mechanisms in Preventing Privilege Escalation Attacks

EDB-ID	CVE-ID	Security Mechanisms				
		Namespace	Cgroup	Capability	Secomp	MAC
Web App Layer						
43002	CVE-2017-15276			●		
40921	CVE-2016-9566			●		
42305	CVE-2017-6970			●		
40938	CVE-2014-6271			●		
Server Layer						
40768	CVE-2016-1247			●		
40678	CVE-2016-6663			●		
40450	CVE-2016-1240			●		
Kernel Layer						
41994	CVE-2017-7388					
43127*						
43029*	CVE-2017-5123					
40871	CVE-2016-8655					
40489						
40435						
44300						
40049	CVE-2016-4997			● NET_ADMIN ¹		
41458	CVE-2017-6074			● NET_ADMIN ¹		
43418	CVE-2017-1000112			● NET_ADMIN ¹		
41995	CVE-2016-9793			● NET_ADMIN ¹		
42887	CVE-2017-1000253			●		
42274	CVE-2017-1000566					
42275	CVE-2017-1000371			●		
42276	CVE-2017-1000379					
	CVE-2017-1000370					
40003					●	
39277	CVE-2016-0728					
39992	CVE-2016-1583			●	●	●
41762	CVE-2017-1575			●	●	●
41763	CVE-2017-1576			●	●	●
39166				●	●	●
39230	CVE-2015-8660			●	●	●
40847						
40616		●		●		
40611	CVE-2016-5195					
40839		●		●	●	
40838		●		●	●	
40759		●		●	●	
39772	CVE-2016-4357			●	●	
41999	CVE-2016-2384	●	●			

^{*} Security mechanism blocks the exploit.

^{*} Exploit bypasses all 5 security mechanisms.

¹ Exploit can achieve privilege escalation when the "NET_ADMIN" capability is included in the *cap_bset* of the caller process. Other exploits marked "•" in "Capability" column can only be successful when all 38 capabilities marked "•" in the *cap_bset*. The "cap_bset" defines the highest privilege a process could reach.

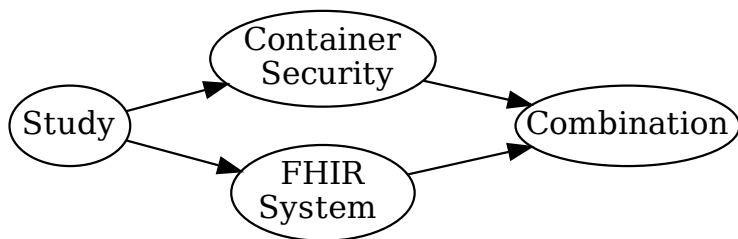
Userland to kernelland

擋掉kernel exploit 可以從無法執行或可執行但不會成功或可執行但會被限制等想法






Interact with FHIR in docker

Current progress

Map-reduce



Map-reduce

- Study:  $\frac{10}{\infty}$
- Container Security:  read some
- FHIR system:  Configured, can run.
- Combination:  Of course: 0
- 專題競賽暨成果展:  $\frac{48}{265} \sim 0.181$

Reference

References I



Xin Lin et al. “A Measurement Study on Linux Container Security: Attacks and Countermeasures”. In: ACSAC '18. San Juan, PR, USA: Association for Computing Machinery, 2018, 418–429. ISBN: 9781450365697. DOI: 10.1145/3274694.3274720. URL: <https://doi.org/10.1145/3274694.3274720>.



S. Wu et al. “Container-Based Cloud Platform for Mobile Computation Offloading”. In: *2017 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*. 2017, pp. 123–132. DOI: 10.1109/IPDPS.2017.47.