Kontejnery a bezpečnost

CryptoFest 2015

Pavel Šnajdr

vpsFree.cz

Kontejnery a bezpečnost

0. Jsou kontejnery bezpečné?
1. Vanilla kontejnery
2. OpenVZ
3. Docker
4. Q/A

whoami

- vpsFree.cz
  - Spoluzakladatel, architekt a admin
  - OpenVZ kontejnery od 2009

Jsou kontejnery bezpečné?

Ano...

Oh wait. Tak jednoduché to nebude...

“Attack surface”

DoS

Privilege escalation
in CT
outside CT

Layers... more layers...

Kontejnery vs. hypervisory

Kontejnery vs. napřímo

Kontejnery pod Linuxem

Vanilla kernel (3.x)

OpenVZ

linux-vserver

Vanilla kernel

Cgroups

Namespaces

Vanilla kernel

Cgroups

cpu
cpuset
memcg
blkio

Vanilla kernel

Namespaces

mnt
UTS
PID
user

Vanilla kernel

PID namespace

Vanilla kernel

User namespace

Capabilities

OpenVZ

2.6.32 -> RHEL6 -> OpenVZ

3.10 -> RHEL7 -> OpenVZ / Virtuozzo 7

OpenVZ

CPU Fairsched

OpenVZ

UBC

kmemsize
socket buffers
numproc
numfile
numiptent

OpenVZ

venet

Docker

Oh well...

Docker

User namespace

Registry Hub

Kernel memory

Network

Docker

OpenVZ to the rescue!

https://github.com/docker/libcontainer/pull/434

“Initial integration of libct into libcontainer”

One more thing...

LSM...

SELinux, AppArmor, TOMOYO, Smack...

One more thing...

... not supported (yet).

Závěr

Jsou kontejnery bezpečné?

Otázky

Anytime -> snajpa@snajpa.net

vpsFree.cz