Tübix 2017

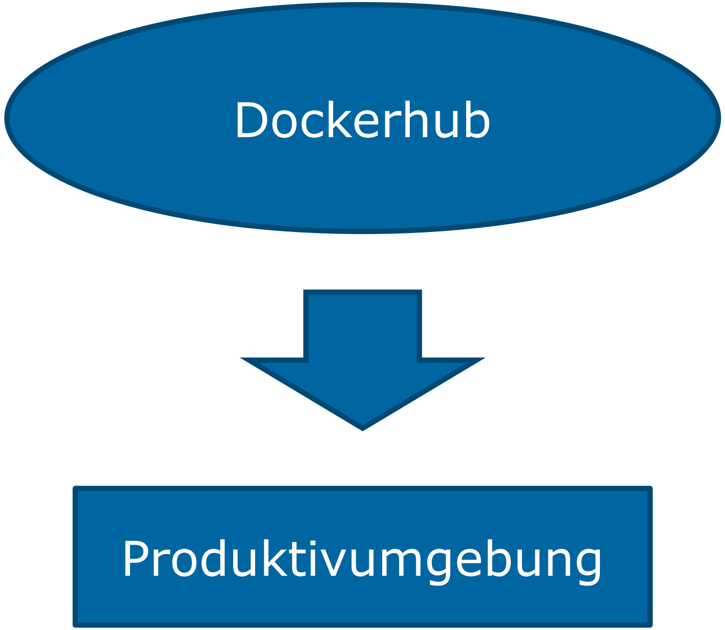
Image-Scanner für Docker

24.06.2017 – Josef Plendl

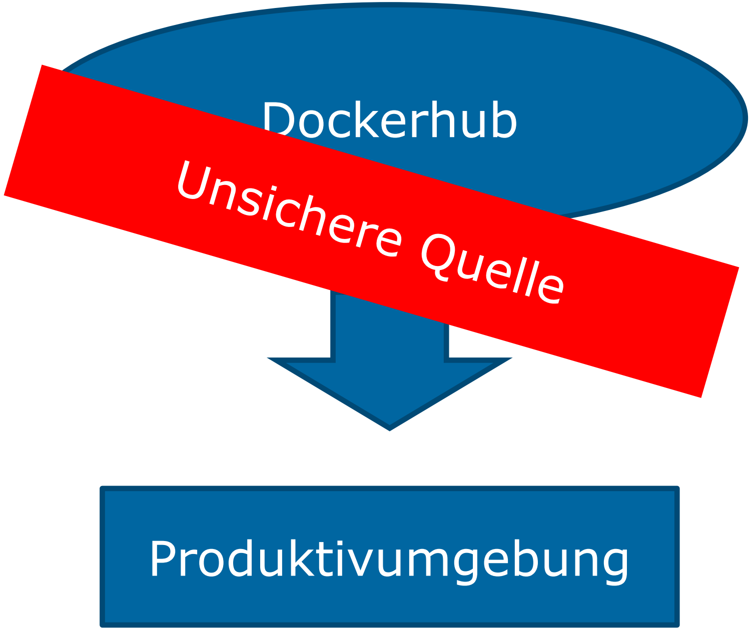
© Atos

Atos

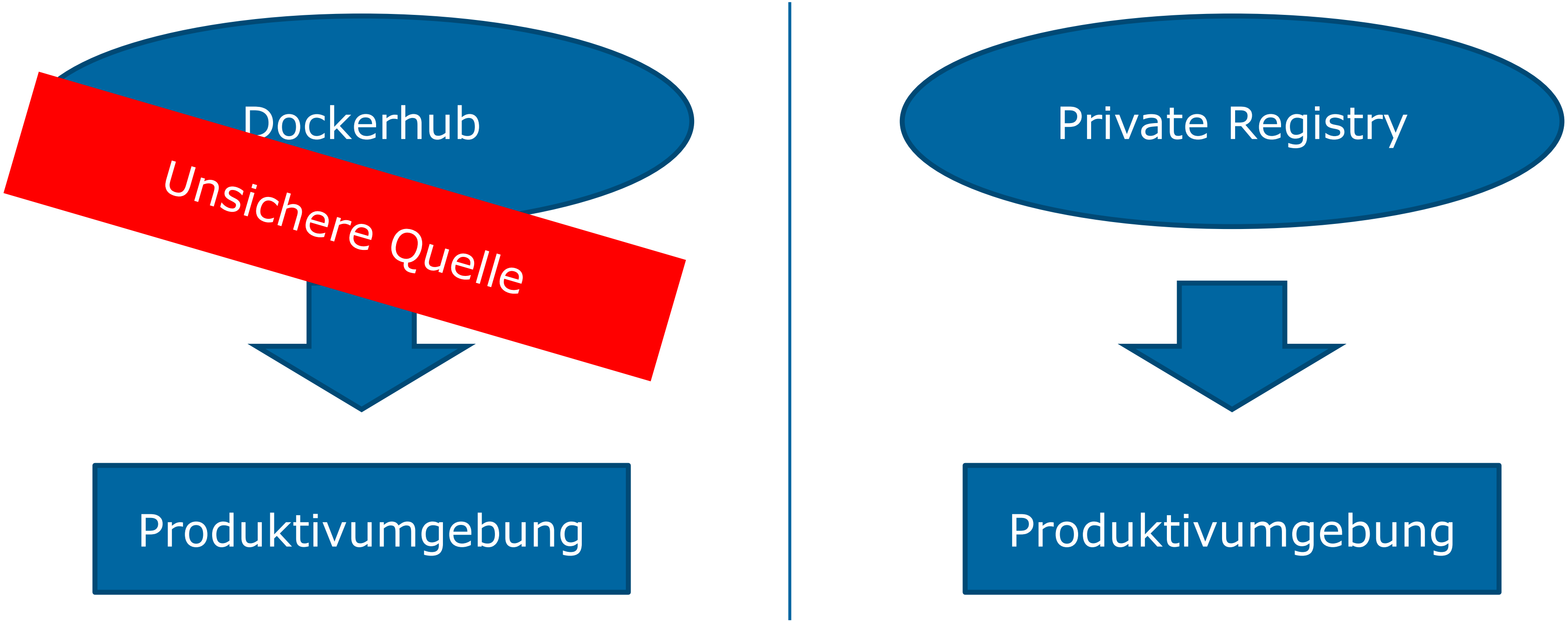
Notwendigkeit



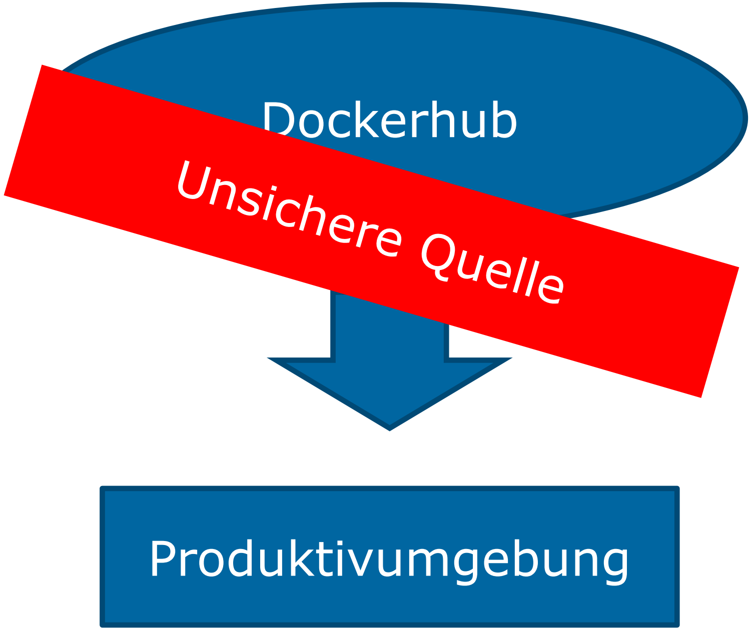
Notwendigkeit

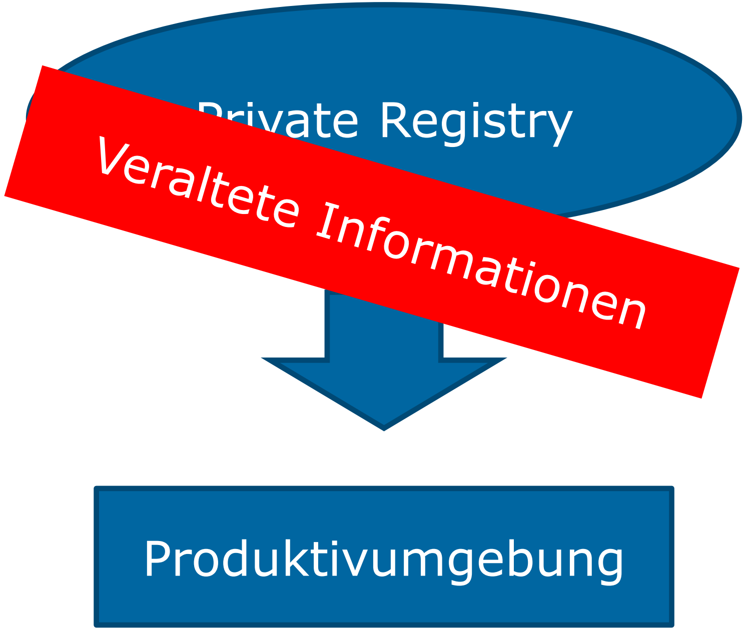


Notwendigkeit



Notwendigkeit





Einschub: Sicherheitslücken

Neue Sicherheitslücke

- Betroffene Hard- / Software
- Auswirkungen / Charakteristika
- Angriffsvektoren
- Risikoeinstufung

Einschub: Sicherheitslücken

Neue Sicherheitslücke

- Betroffene Hard- / Software
- Auswirkungen / Charakteristika
- Angriffsvektoren
- Risikoeinstufung

CVE-2017-0144

Einschub: Sicherheitslücken

Neue Sicherheitslücke

- ▶ Betroffene Hard- / Software
- ▶ Auswirkungen / Charakteristika
- ▶ Angriffsvektoren
- ▶ Risikoeinstufung

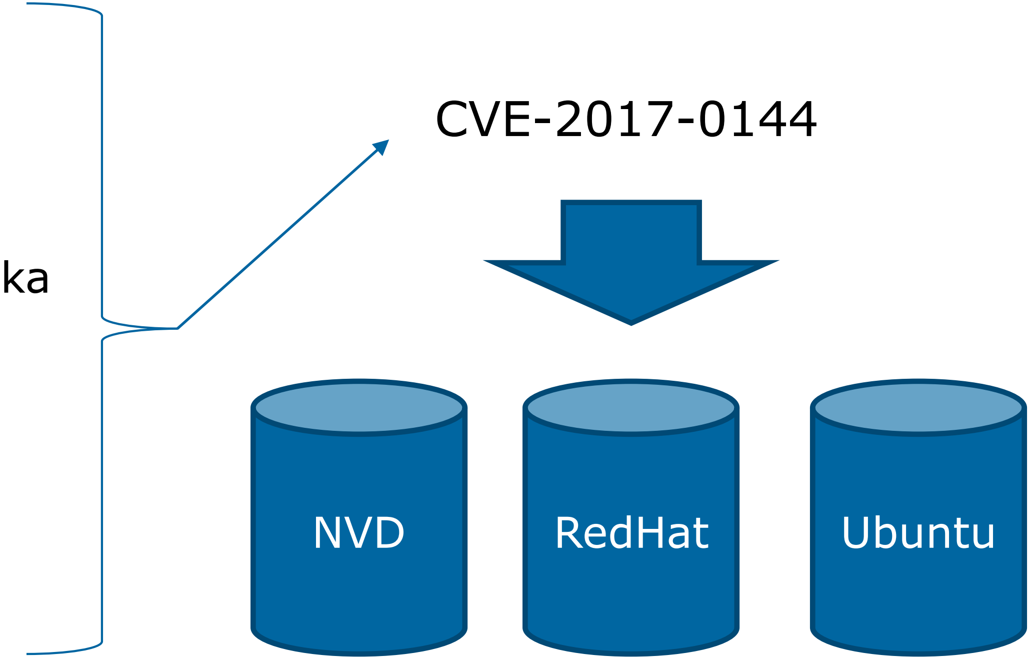


Image-Scanner

Docker: Security Scan

- Docker Cloud
- Docker Hub

Image-Scanner

Docker: Security Scan

- Docker Cloud
- Docker Hub

CoreOS: Clair

- Quay.io / Enterprise
- Dockyard
- Clairctl
- Klar
- Reg

Image-Scanner

Docker: Security Scan

- Docker Cloud
- Docker Hub

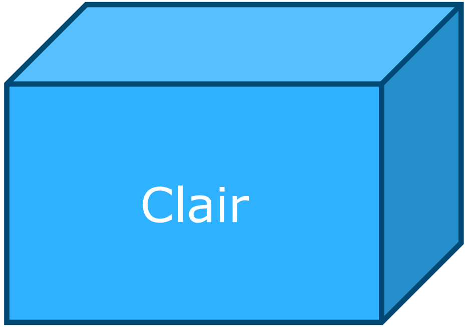
CoreOS: Clair

- Quay.io / Enterprise
- Dockyard
- Clairctl
- Klar
- Reg

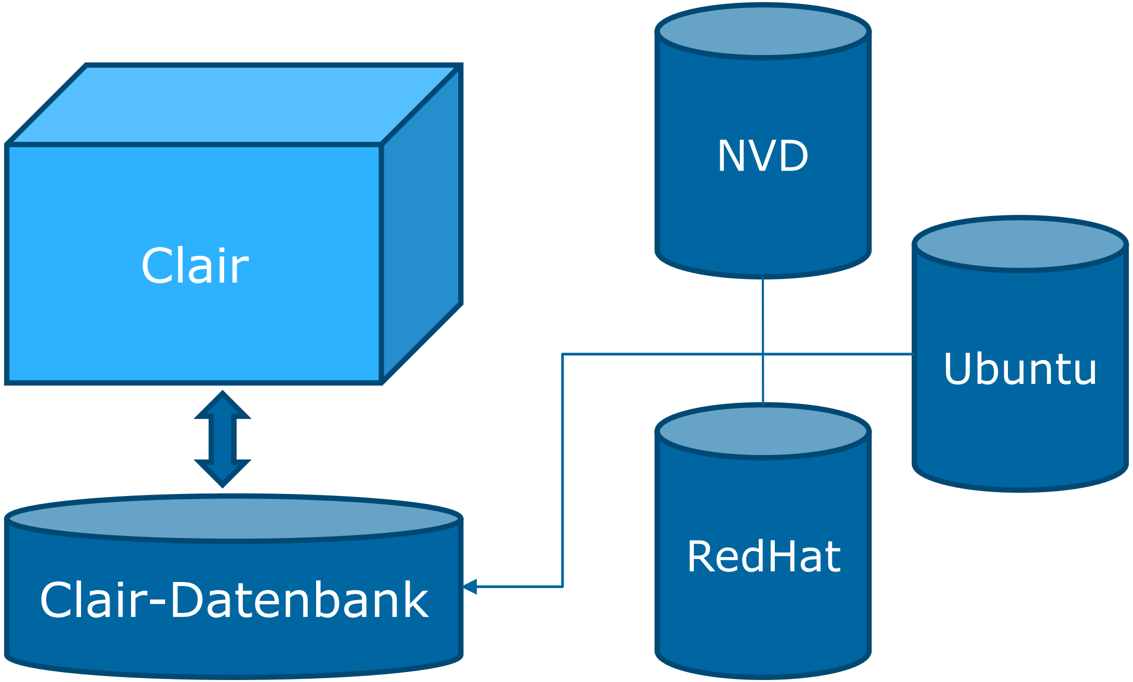
RedHat: Atomic Scan

IBM: Vulnerability Advisor

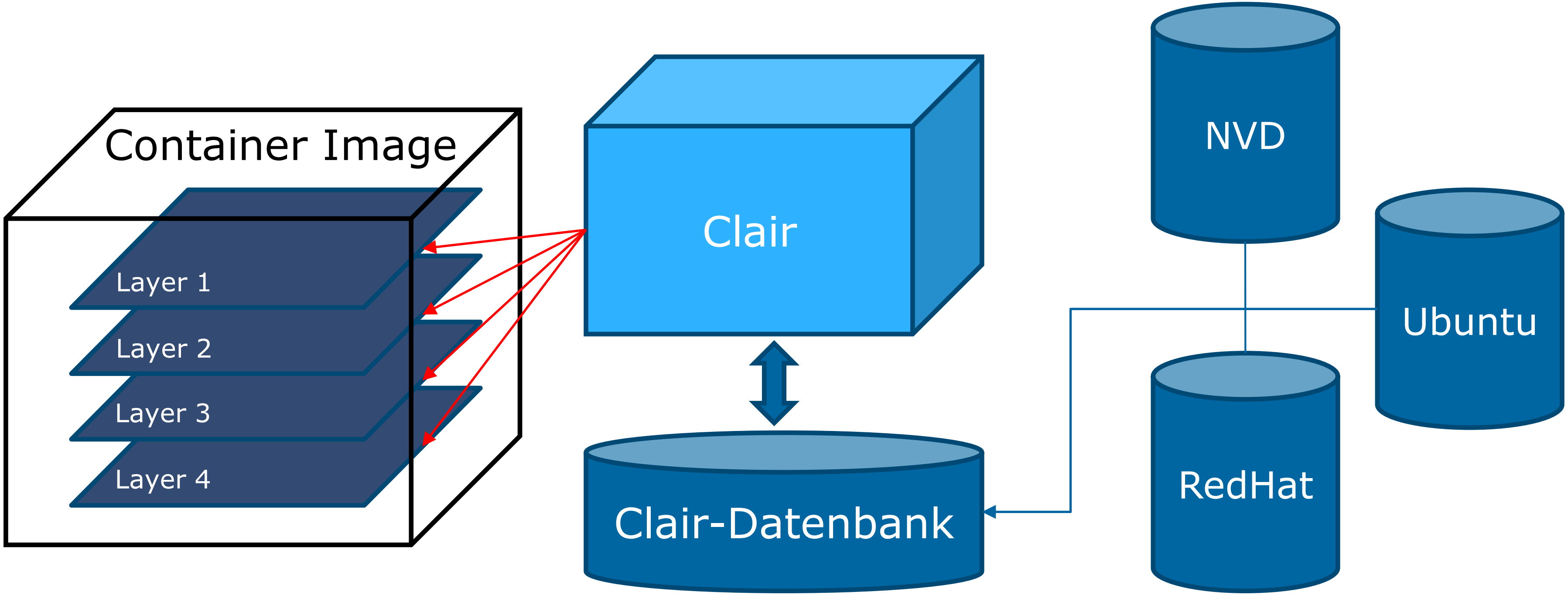
Clair



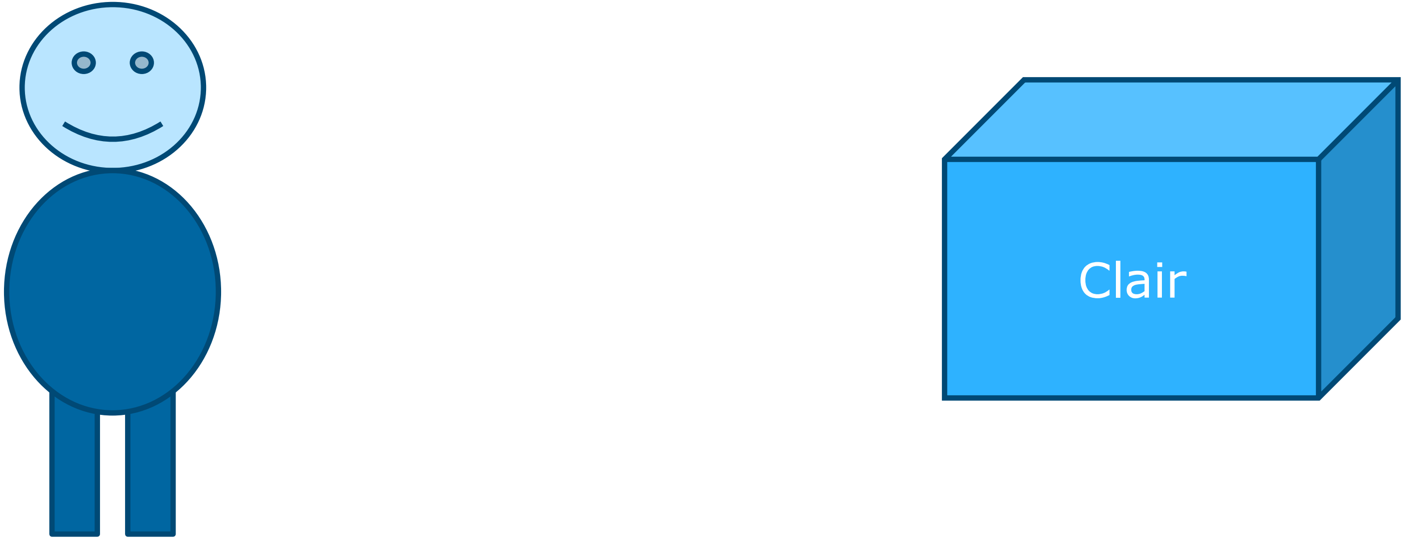
Clair



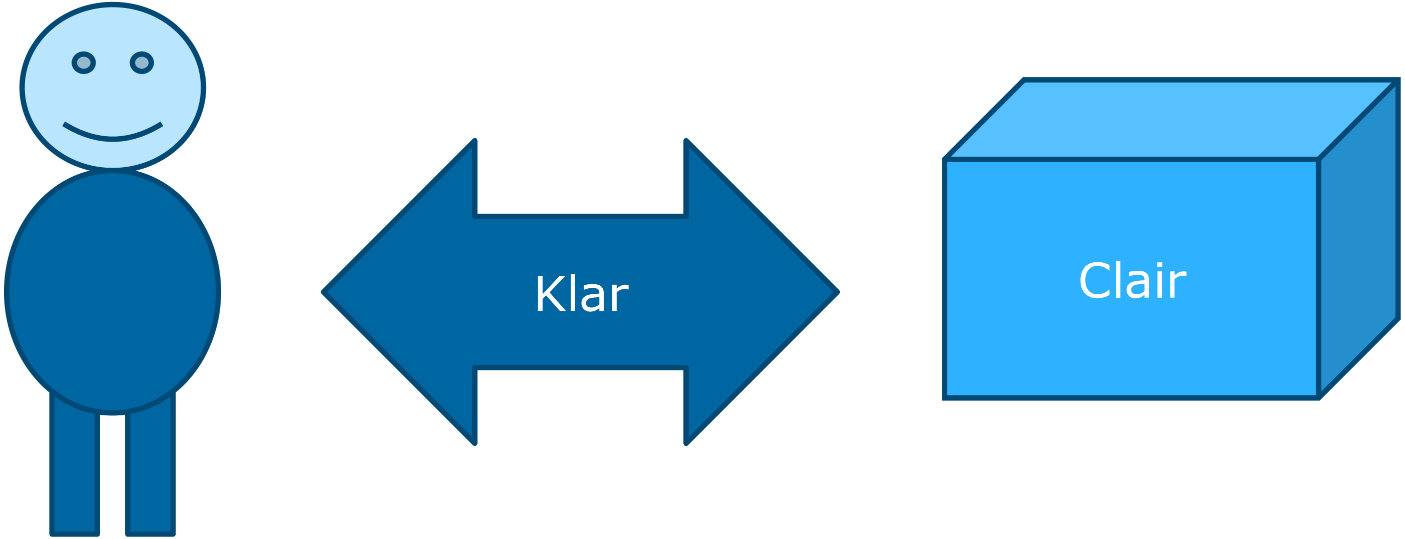
Clair


Container Image
Layer 1
Layer 2
Layer 3
Layer 4
Clair
Clair-Datenbank
NVD
Ubuntu
RedHat

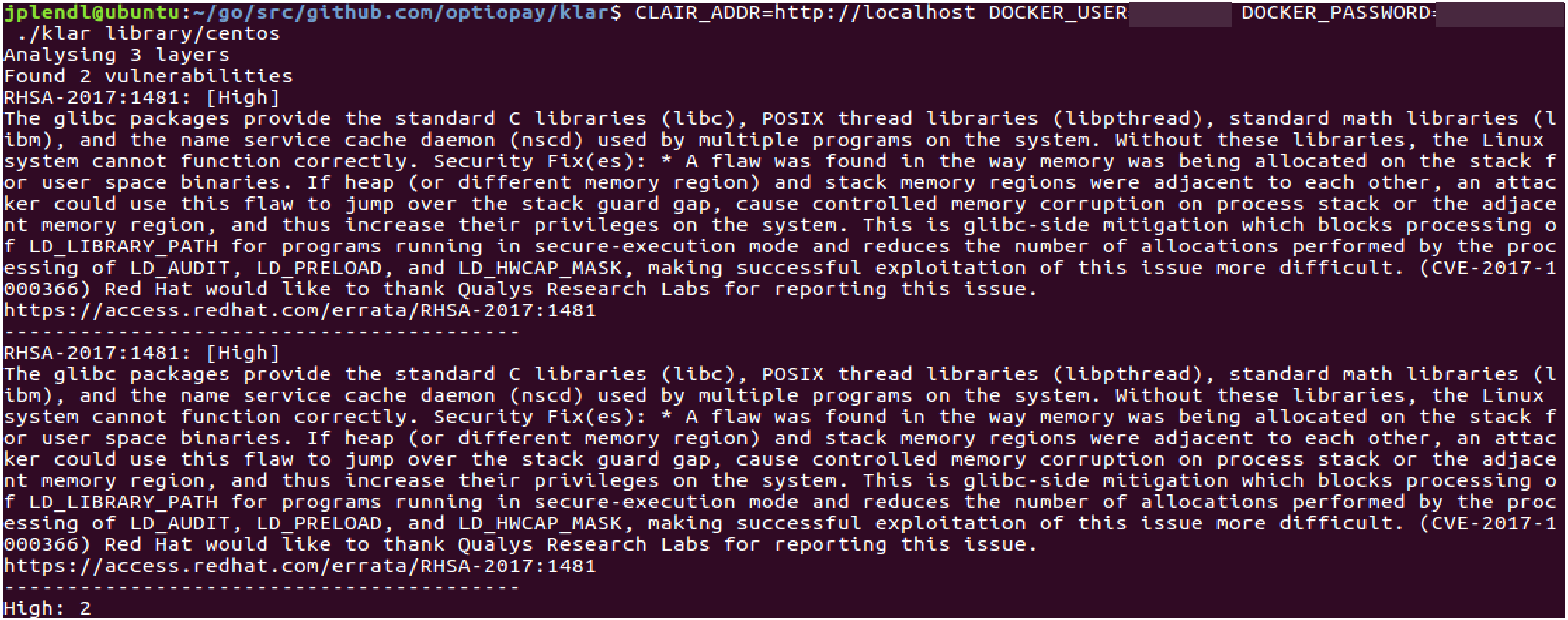
Klar



Klar



Clair/Klar Scan



```
jplendl@ubuntu:~/go/src/github.com/optiopay/klar$ CLAIR_ADDR=http://localhost DOCKER_USER[redacted] DOCKER_PASSWORD=[redacted]
 ./klar library/centos
Analysing 3 layers
Found 2 vulnerabilities
RHSA-2017:1481: [High]
The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (l
ibm), and the name service cache daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux
system cannot function correctly. Security Fix(es): * A flaw was found in the way memory was being allocated on the stack f
or user space binaries. If heap (or different memory region) and stack memory regions were adjacent to each other, an attac
ker could use this flaw to jump over the stack guard gap, cause controlled memory corruption on process stack or the adjace
nt memory region, and thus increase their privileges on the system. This is glibc-side mitigation which blocks processing o
f LD_LIBRARY_PATH for programs running in secure-execution mode and reduces the number of allocations performed by the proc
essing of LD_AUDIT, LD_PRELOAD, and LD_HWCAP_MASK, making successful exploitation of this issue more difficult. (CVE-2017-1
000366) Red Hat would like to thank Qualys Research Labs for reporting this issue.
https://access.redhat.com/errata/RHSA-2017:1481
-----------------------------------------
RHSA-2017:1481: [High]
The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (l
ibm), and the name service cache daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux
system cannot function correctly. Security Fix(es): * A flaw was found in the way memory was being allocated on the stack f
or user space binaries. If heap (or different memory region) and stack memory regions were adjacent to each other, an attac
ker could use this flaw to jump over the stack guard gap, cause controlled memory corruption on process stack or the adjace
nt memory region, and thus increase their privileges on the system. This is glibc-side mitigation which blocks processing o
f LD_LIBRARY_PATH for programs running in secure-execution mode and reduces the number of allocations performed by the proc
essing of LD_AUDIT, LD_PRELOAD, and LD_HWCAP_MASK, making successful exploitation of this issue more difficult. (CVE-2017-1
000366) Red Hat would like to thank Qualys Research Labs for reporting this issue.
https://access.redhat.com/errata/RHSA-2017:1481
-----------------------------------------
High: 2
```

Vielen Dank

Ansprechpartner für weitere Informationen:

Josef Plendl
T +49 7071 9457-312
josef.plendl@atos.net

Atos, das Atos Logo, Atos Codex, Atos Consulting, Atos Worldgrid, Worldline, BlueKiwi, Bull, Canopy the Open Cloud Company, Unify, Yunano, Zero Email, Zero Email Certified und The Zero Email Company sind eingetragene Warenzeichen der Atos Gruppe. April 2016. © 2016 Atos. Die Informationen sind vertraulich und Eigentum von Atos. Sie dürfen nur vom Empfänger genutzt werden. Dieses Dokument darf weder ganz noch teilweise reproduziert, kopiert, in Umlauf gebracht, verteilt oder zitiert werden, ohne dass hierfür eine schriftliche Genehmigung von Atos vorliegt.

Bild- und Textquellen

Quellen
Bildquellen:
https://cloud.githubusercontent.com/assets/343539/21630811/c5081e5c-d202-11e6-92eb-919d5999c77a.png
https://kleewald.eu/wp-content/uploads/2017/04/docker_logo.png
http://community.redhat.com/images/branding/logo-atomic.png?1461773619
Textquellen:
https://cve.mitre.org/
https://nvd.nist.gov/
https://github.com/coreos/clair
https://github.com/optiopay/klar