Building confidence via automated container security scanning

XAVIER VELLO

Software Engineer, Datadog

DATADOG

Saas Monitoring

Metrics, APM, Logs, Synthetics

We are hiring

Why?

- Agent is installed on the monitored hosts, broad access
- 9,000+ customers, security is paramount
- Polyglot codebase (Go + Python + Java)
- Be proactive and transparent

What?

Scan rules

- Known CVEs*
- Good practices
- Custom compliance rules

+

Image contents

- Installed OS packages
- Language-specific packages (python, java…)
- File hashes & types

→

Image scan results

- Vulnerabilities (by severity)
- Compliance issues
- Yes/no signal based on acceptable severity

* CVE: Common Vulnerabilities and Exposures

Step 0: Manual scans

Manual workflow

```
$ docker push myregistry/datadog/agent:rc1
$ sleep 600
$ open https://myregistry/scan_results
```

LAST PUSHED	VULNERABILITIES	LAST MODIFIED	SECURITY SCAN
12 minutes ago by datadog	Scanning...	10 minutes ago	Queued

Step 1:

- Automated scans
- Manual processing

Automating the scans

- Scanners watch the datadog/* Docker Hub repos
- Use our Gitlab CI to push images to scanners
- After building RC1, look at the scan results

Automated registry scanning

Monitor / Vulnerabilities

Vulnerability Explorer | Images | Hosts | Registry | Serverless | Jenkins Jobs | Twist

CSV | Search registry | Collections | Scar

Registry	Repository	Tag	Vulnerabilities	Compliance
docker.io	datadog/agent	latest-jmx	6 14	0
docker.io	datadog/agent-dev	master-jmx	6 13	0
docker.io	datadog/cluster-agent	latest	3 5	0
docker.io	datadog/cluster-agent...	master	1 5	0
docker.io	datadog/agent-dev	master	1 5	0
docker.io	datadog/agent	latest	1 5	0
docker.io	datadog/dogstatsd-dev	master	0	0
docker.io	datadog/dogstatsd	latest	0	0

Automated registry push

```
dev_master_quay:
  <<: *docker_tag_job_definition
  <<: *run_when_triggered_on_nightly
  variables:
    <<: *quay_variables
  script:
    - publish ${SRC_AGENT}:${SRC_TAG} quay.io/dd/agent-dev:master
    - publish ${SRC_AGENT}:${SRC_TAG}-jmx quay.io/dd/agent-dev:master-jmx
    - publish ${SRC_DSD}:${SRC_TAG} quay.io/dd/dogstatsd-dev:master
    - publish ${SRC_DCA}:${SRC_TAG} quay.io/dd/cluster-agent-dev:master
```

Does not scale

4

agent
agent-jmx
dogstatsd
cluster-agent

x

4

Aqua
Clair
DTR
Twistlock

x

2

Latest
Master

= 32

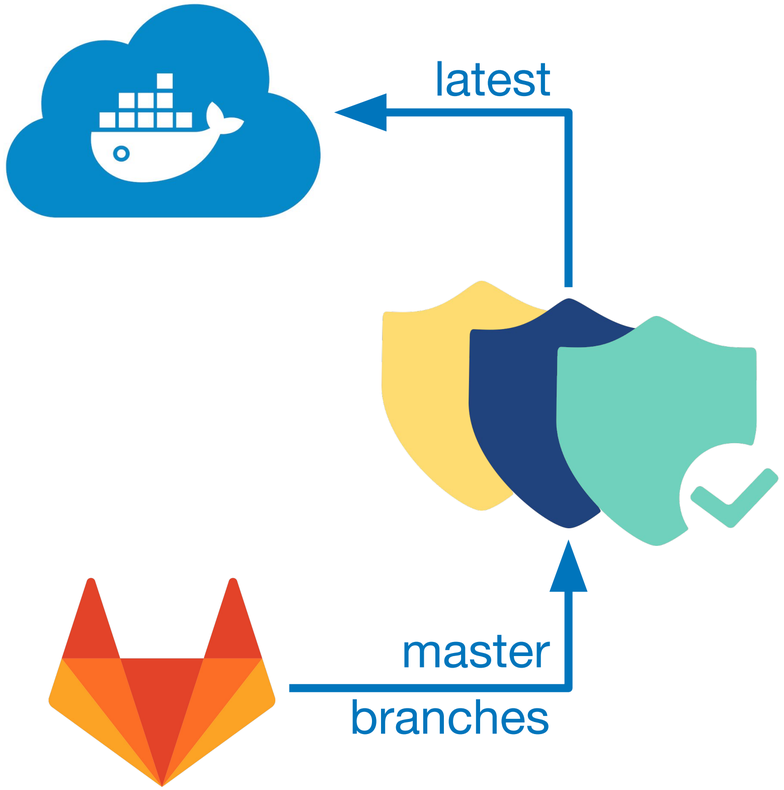
RC1 is too late

- Might delay the release
- Possible side effects

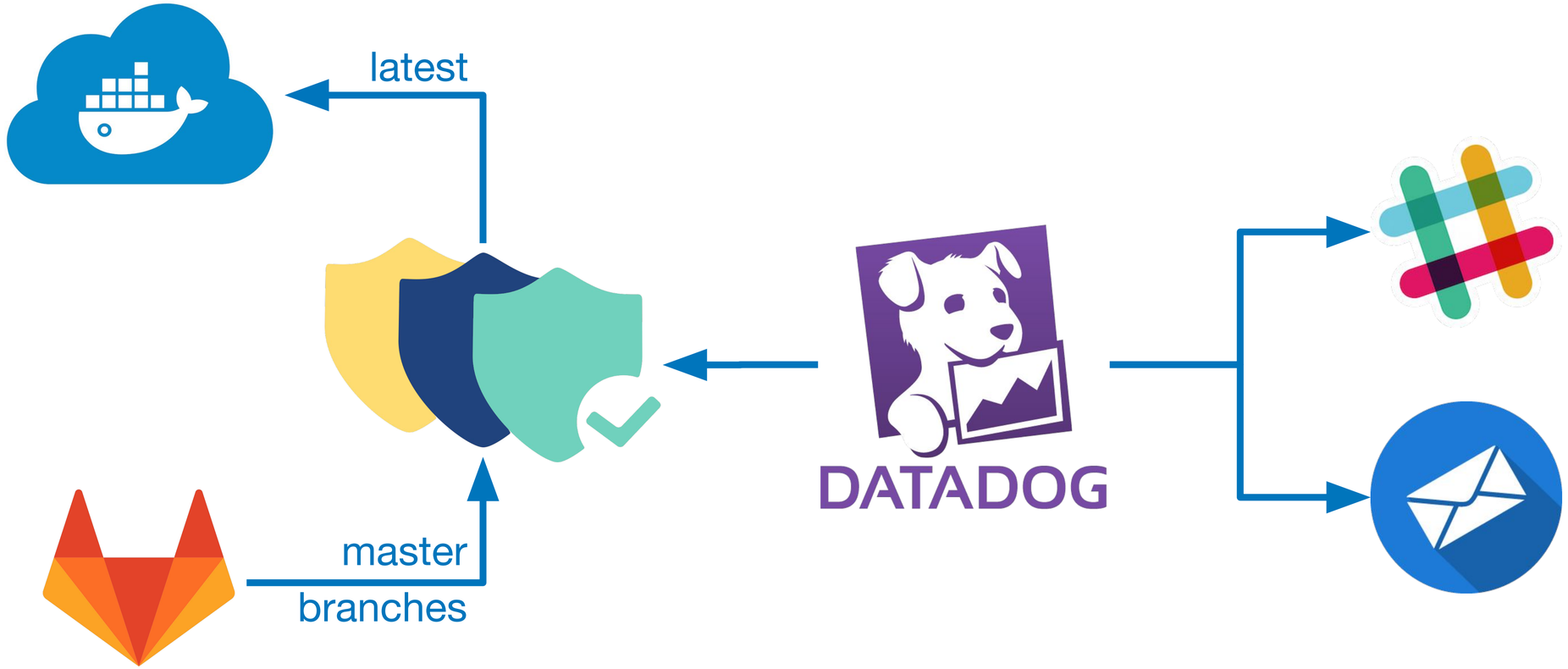
Step 2:

- Automated scans
- Automated alerting

Our automated pipeline



Our automated pipeline



```python
class Twistlock(AgentCheck):
    NAMESPACE = 'twistlock'

    def check(self, instance):
        if 'url' not in instance:
            raise Exception('Instance missing "url" value.')
        self._report_registry_scan(instance)

    def _retrieve_json(self, instance, path):
        base_url = instance.get('url')
        user = instance.get('user')
        password = instance.get('password')
        return requests.get(base_url + path, auth=(user, password), verify=False).json()

    def _report_registry_scan(self, instance):
        namespace = self.NAMESPACE + ".registry"
        service_check_name = self.NAMESPACE + ".can_connect"
        instance_tags = instance.get('tags') or []
        try:
            scan_result = self._retrieve_json(instance, "/api/v1/registry")
            self.service_check(service_check_name, AgentCheck.OK)
        except Exception as e:
            self.warning("cannot retrieve registry data: %s", e)
            self.service_check(service_check_name, AgentCheck.CRITICAL)
            return None

        current_date = datetime.now()
        warning_date = current_date - timedelta(hours=7)
        critical_date = current_date - timedelta(days=1)

        for image in scan_result:
            if '_id' not in image:
                continue
            image_name = image['_id']
            if image_name.startswith(DOCKERIO_PREFIX):
                image_name = image_name[len(DOCKERIO_PREFIX):]
            image_tags = ["scanned_image:" + image_name] + instance_tags

            # Layer count and size
            layer_count = 0
            layer_sizes = 0
            for layer in image.get('info', {}).get('history', []):
                layer_count += 1
                layer_sizes += layer.get('sizeBytes', 0)
            self.gauge(namespace + '.image.size', float(layer_sizes), image_tags)
            self.gauge(namespace + '.image.layer_count', float(layer_count), image_tags)

            # Last scan service check
            scan_date = datetime.strptime(image.get("scanTime"), SCAN_DATE_FORMAT)
            scan_status = AgentCheck.OK
            if scan_date < warning_date:
                scan_status = AgentCheck.WARNING
            if scan_date < critical_date:
                scan_status = AgentCheck.CRITICAL
            self.service_check(namespace + '.image.is_scanned', scan_status,
                               tags=image_tags, message="Last scan: " + image.get("scanTime"))

            # CVE vulnerabilities
            summary = Counter({"critical": 0, "high": 0, "medium": 0, "low": 0})
            cves = image.get('info', {}).get('cveVulnerabilities', []) or []
            for cve in cves:
                summary[cve['severity']] += 1
                tags = [
                    'cve:' + cve['cve'],
                ] + SEVERITY_TAGS.get(cve['severity'], []) + image_tags
                if 'packageName' in cve:
                    tags += ["package:" + cve['packageName']]
                self.gauge(namespace + '.image.cve.details', float(1), tags)

            # Send counts to avoid no-data on zeroes
            for severity, count in summary.iteritems():
                tags = SEVERITY_TAGS.get(severity, []) + image_tags
                self.gauge(namespace + '.image.cve.count', float(count), tags)
```

docker con 18 EUROPE

Twistlock scan results

Edit Board

1mo The Past Month

$env build-stable | $min_severity high | $image datadog/cluster-agent-dev:master

Up-to-date scans	Active consoles
8	1

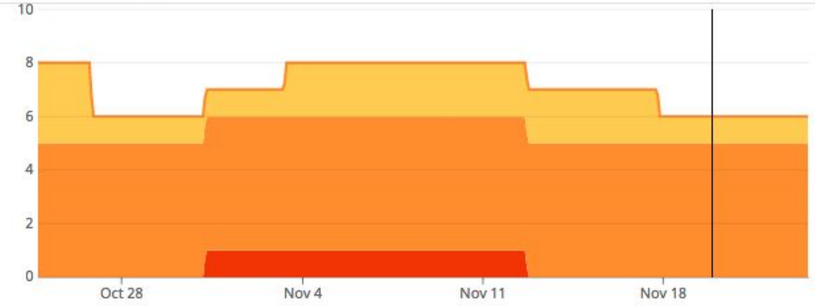
Monitors status

STATUS	NAME
OK	Twistlock: TLS certificate expiration
OK	Twistlock high/critical vulnerabilities
OK	Twistlock scans falling behind
OK	Twistlock gitlab CI scan failing on mast...
OK	Twistlock licence will expire soon

Images with vuln higher than $min_severity

0.00	datadog/agent-dev:master
0.00	datadog/cluster-agent:latest
0.00	datadog/dogstatsd:latest
0.00	datadog/agent:latest-jmx
0.00	datadog/agent-dev:master-jmx
0.00	datadog/agent:latest
0.00	datadog/cluster-agent-dev:master
0.00	datadog/dogstatsd-dev:master

CVEs by severity



Affected packages for $min_severity

6.00	libtasn1-6

Affected package for $min_severity and $image

1.00	libtasn1-6

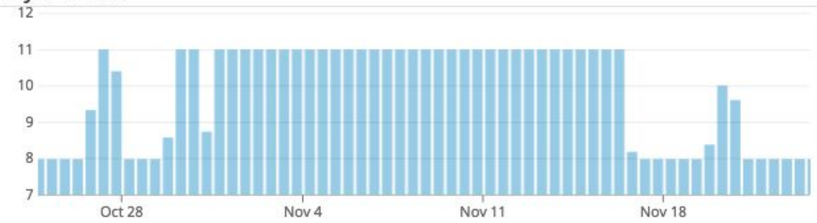
Uncompressed image size

nebibytes

525.88	datadog/agent-dev:master-jmx
498.27	datadog/agent:latest-jmx
381.95	datadog/agent-dev:master
354.41	datadog/agent:latest
139.22	datadog/cluster-agent-dev:master
137.31	datadog/cluster-agent:latest
16.94	datadog/dogstatsd-dev:master
16.93	datadog/dogstatsd:latest

Uncompressed image size

Layer count



dockercon18 EUROPE

OK Monitor status since 1 week and 3 days ago (12 Nov, 11:50:57 EST)

Mute

Twistlock high/critical vulnerabilities

Properties

Metric Monitor
ID: 6345115

Created by Xavier Vello

TAGS

team:container-integrations
service:twistlock

QUERY

```
avg(last_5m):sum:twistlock.registry.image.cve.count{min_severity:high,env:
build-stable} by {scanned_image,env} > 0
```

MESSAGE
2 notified

See scan results: https://app.datadoghq.com/screen/445585/twistlock-scan-results?tpl_var_image={{scanned_image.name}}&tpl_var_env={{env.name}}
@xavier.vello@datadoghq.com @slack-Main_Account-container-scans

Slack Main_Account container-scans Xavier Vello

Filter monitor groups and their events...

Alert 0 Warn 0 No Data 0 OK 8 **8 of 8 groups** 4h The Past 4 Hours

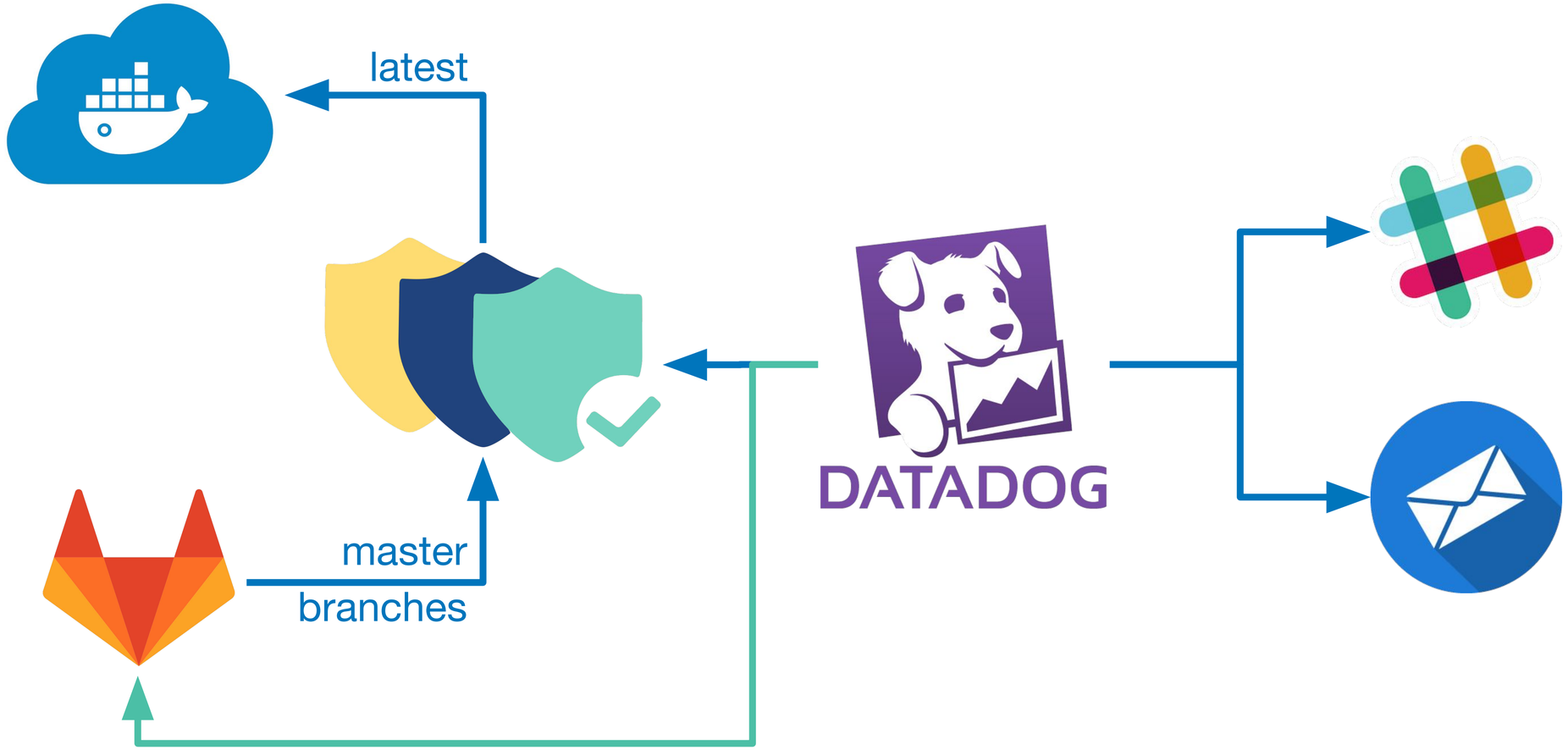
Status & History

GROUP STATUS **Showing 5 of 8 groups** 1 2 Sort by Triggered ↓

NAME	VALUE	UPTIME
env:build-stable,scann...	0	100.0%
env:build-stable,scann...	0	100.0%
env:build-stable,scann...	0	100.0%
env:build-stable,scann...	0	100.0%
env:build-stable,scann...	0	100.0%

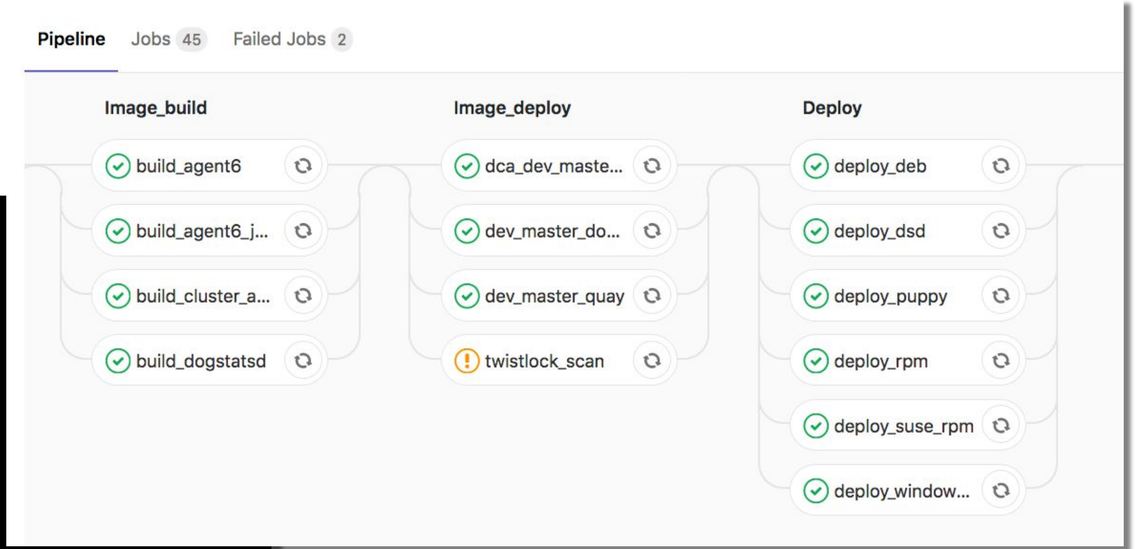
docker con 18 EUROPE

Our automated pipeline



Automated CI scans

```yaml
twistlock_scan:
  stage: image_deploy
  tags: [ "runner:docker", "size:large" ]
  image: REGISTRY/twistlock-cli:2.5.121
  dependencies: [] # Don't download Gitlab artefacts
  allow_failure: true # Don't block the pipeline
  before_script:
    - export SRC_TAG=v$CI_PIPELINE_ID-${CI_COMMIT_SHA:0:7}
  script:
    - scan datadog/agent:${SRC_TAG}
    - scan datadog/agent:${SRC_TAG}-jmx
    - scan datadog/dogstatsd:${SRC_TAG}
    - scan datadog/cluster-agent:${SRC_TAG
```




```bash
scan () {
    echo -e "\n==== Scanning $1 ====\n";
    docker pull $1 > /dev/null;
    /twistcli images scan --address="$TWISTLOCK_URL" $1;
}
```

OK Monitor status since 3 weeks ago (7 Nov, 14:25:09 EST)

Mute

Twistlock gitlab CI scan failing on master

Properties

Metric Monitor
ID: 6963905

Created by Xavier Vello

TAGS
service:twistlock
team:container-integrations

QUERY

```
sum(last_1d):sum:gitsync.statuses.failed{env:build-stable,job:dd-gitlab/twistlock_scan,branch_type:prod}.
as_count() > 0
```

MESSAGE
1 notified

https://gitlab.ddbuild.io/DataDog/datadog-agent/commits/master **@slack-Main_Account-container-scans**

Slack Main_Account container-scans

Filter monitor groups and their events...

Alert 0 | Warn 0 | No Data 0 | OK 1 | **1 of 1 groups**

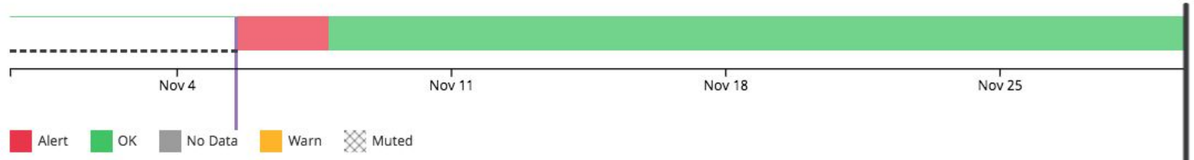
1M 30 Oct, 5:51pm - 29 Nov, 5:51pm

Status & History

GROUP STATUS

Showing 1 of 1 groups Sort by Triggered ↓

NAME	VALUE	UPTIME
* (Entire Infrastructure)	#	92.3%



HISTORY

2h

docker con 18 EUROPE

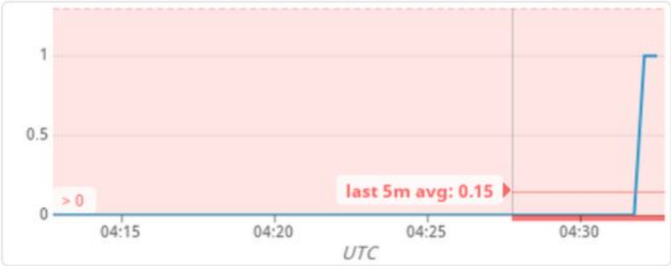
Response to a new vulnerability

New CVE alert

Wednesday, October 31st

Datadog APP 05:33

Triggered: Twistlock high/critical vulnerabilities on env:build-stable,scanned_image:datadog/cluster-agent:latest (6 kB)



Pipeline Jobs 45 Failed Jobs 2

Image_build	Image_deploy	Deploy
build_agent6	dca_dev_maste...	deploy_deb
build_agent6_j...	dev_master_do...	deploy_dsd
build_cluster_a...	dev_master_quay	deploy_puppy
build_dogstatsd	twistlock_scan	deploy_rpm
		deploy_suse_rpm
		deploy_window...

DATADOG

Watchdog
Events
Dashboards
Infrastructure
Monitors
Metrics
Integrations
APM
Notebooks
Logs
Synthetics
Help
Team
xavier.vello (Datadog HQ)

Twistlock scan results

3 d Oct 30, 12:00AM - Nov 1, 11:59PM

$env build-stable | $min_severity high | $image datadog/agent:latest-jmx

Aggregated results

Images with vuln higher than $min_severity

1.00	datadog/agent-dev:master
1.00	datadog/cluster-agent:latest
1.00	datadog/agent:latest-jmx
1.00	datadog/agent-dev:master-jmx
1.00	datadog/agent:latest
1.00	datadog/cluster-agent-dev:master
0.00	datadog/dogstatsd:latest
0.00	datadog/dogstatsd-dev:master

Affected packages for $min_severity

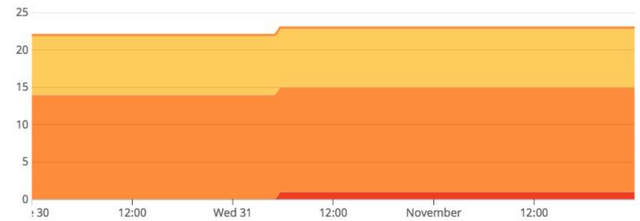
6.00	libtasn1-6

Uncompressed image size (mebibytes)

514.83	datadog/agent-dev:master-jmx
496.83	datadog/agent:latest-jmx
370.95	datadog/agent-dev:master
353.53	datadog/agent:latest
138.06	datadog/cluster-agent-dev:master
137.31	datadog/cluster-agent:latest
16.93	datadog/dogstatsd-dev:master
16.93	datadog/dogstatsd:latest

Per-image results

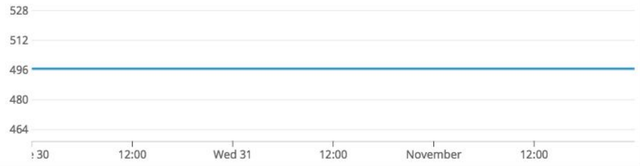
CVEs by severity



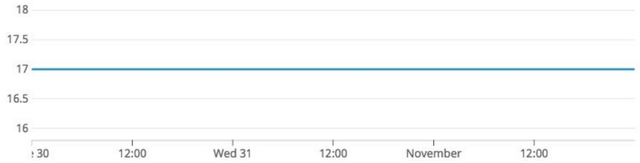
Affected package for $min_severity and $image

1.00	libtasn1-6

Uncompressed image size



Layer count



dockercon18 EUROPE

Investigating

Id	Type	Highest Severity	Description
46	OS	high	libtasn1-6 version 4.13-3 has 1 vulnerability. Hide details

Severity	Package	CVE	Vendor Status	Risk Factors	Description
high	libtasn1-6	CVE-2018-1000654	open	3	GNU Libtasn1-4.13 libtasn1-4.13 version libtasn1-4.13, libtasn1-4.1 2 contains a DoS, specifically CPU usage will reach 100% when running asn1Paser against the POC due to an issue in _asn1_ex pand_object_id(p_tree), after a long time, the program will be k illed. This attack appears to be exploitable via parsing a crafted file.

46	OS	medium	passwd (shadow) version 1:4.5-1.1 has 1 vulnerability. Show details
46	OS	medium	login (shadow) version 1:4.5-1.1 has 1 vulnerability. Show details
46	OS	medium	libdb5.3 (db5.3) version 5.3.28+dfsg1-0.2 has 1 vulnerability. Show details
46	OS	medium	libc6 (glibc) version 2.27-6 has 1 vulnerability. Show details
46	OS	medium	libc-bin (glibc) version 2.27-6 has 1 vulnerability. Show details

Investigating

Id	Type	Highest Severity	Description
46	OS	high	libtasn1-6 version 4.13-3 has 1 vulnerability. Hide details

Severity	Package	CVE	Vendor Status	Risk Factors	Description
high	libtasn1-6	CVE-2018-1000654	open	3	GNU Libtasn1-4.13 libtasn1-4.13 version libtasn1-4.13, libtasn1-4.12 contains a DoS, specifically CPU usage will reach 100% when running asn1Paser against the POC due to an issue in _asn1_expand_object_id(p_tree), after a long time, the program will be killed. This attack appears to be exploitable via parsing a crafted file.

sswd (shadow) version 1:4.5-1.1 has 1 vulnerability. Show details

gin (shadow) version 1:4.5-1.1 has 1 vulnerability. Show details

db5.3 (db5.3) version 5.3.28+dfsg1-0.2 has 1 vulnerability. Show details

c6 (glibc) version 2.27-6 has 1 vulnerability. Show details

c-bin (glibc) version 2.27-6 has 1 vulnerability. Show details

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
libtasn1-6 (PTS)	jessie, jessie (security)	4.2-3+deb8u3	vulnerable
	stretch, stretch (security)	4.10-1.1+deb9u1	vulnerable
	buster, sid	4.13-3	vulnerable

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

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
libtasn1-3	source	(unstable)	(unfixed)	high		
libtasn1-6	source	(unstable)	(unfixed)	high		906768

Notes

```
[stretch] - libtasn1-6 <no-dsa> (Minor issue)
[jessie] - libtasn1-6 <no-dsa> (Minor issue since this cannot be exploited at runtime)
https://gitlab.com/gnutls/libtasn1/issues/4
```

Investigating

Id	Type	Highest Severity	Description
46	OS	high	libtasn1-6 version 4.13-3 has 1 vulnerability. Hide details

Severity	Package	CVE	Vendor Status	Risk Factors	Description
high	libtasn1-6	CVE-2018-1000654	open	3	GNU Libtasn1-4.13 libtasn1-4.13 version libtasn1-4.13, libtasn1-4.1 2 contains a DoS, specifically CPU usage will reach 100% when running asn1Paser against the POC due to an issue in _asn1_ex pand_object_id(p_tree), after a long time, the program will be k

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
libtasn1-6 (PTS)	jessie, jessie (security)	4.2-3+deb8u3	vulnerable
	stretch, stretch (security)	4.10-1.1+deb9u1	vulnerable
	buster, sid	4.13-3	vulnerable

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

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
libtasn1-3	source	(unstable)	(unfixed)	high		
libtasn1-6	source	(unstable)	(unfixed)	high		906768

Notes

```
[stretch] - libtasn1-6 <no-dsa> (Minor issue)
[jessie] - libtasn1-6 <no-dsa> (Minor issue since this cannot be exploited at runtime)
https://gitlab.com/gnutls/libtasn1/issues/4
```

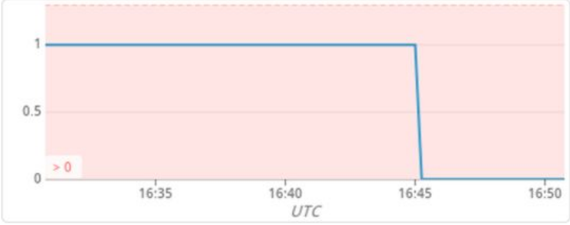
```
$ docker run --rm -it datadog/agent bash

What depends on the library package?

root@agent:/# apt-get remove libtasn1-6
...
The following packages will be REMOVED:
  apt apt-file libgnutls30 libtasn1-6

Vulnerable binary is asn1Parser, what package ships it?

root@agent:/# apt-file search /usr/bin/asn1Parser
libtasn1-bin: /usr/bin/asn1Parser

Is it installed in our images?

root@agent:/# dpkg -l | grep tasn
ii  libtasn1-6:amd64 4.13-3 amd64
Manage ASN.1 structures (runtime)
```

Alert recovery

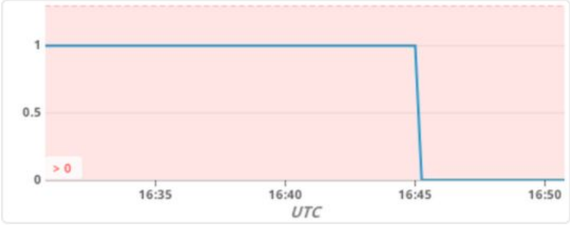
Datadog APP 20:25
Recovered: Twistlock gitlab CI scan failing on master

Datadog APP 17:51

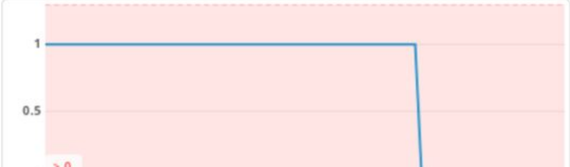
Recovered: Twistlock high/critical vulnerabilities on env:build-stable,scanned_image:datadog/agent:latest-jmx (4 kB)

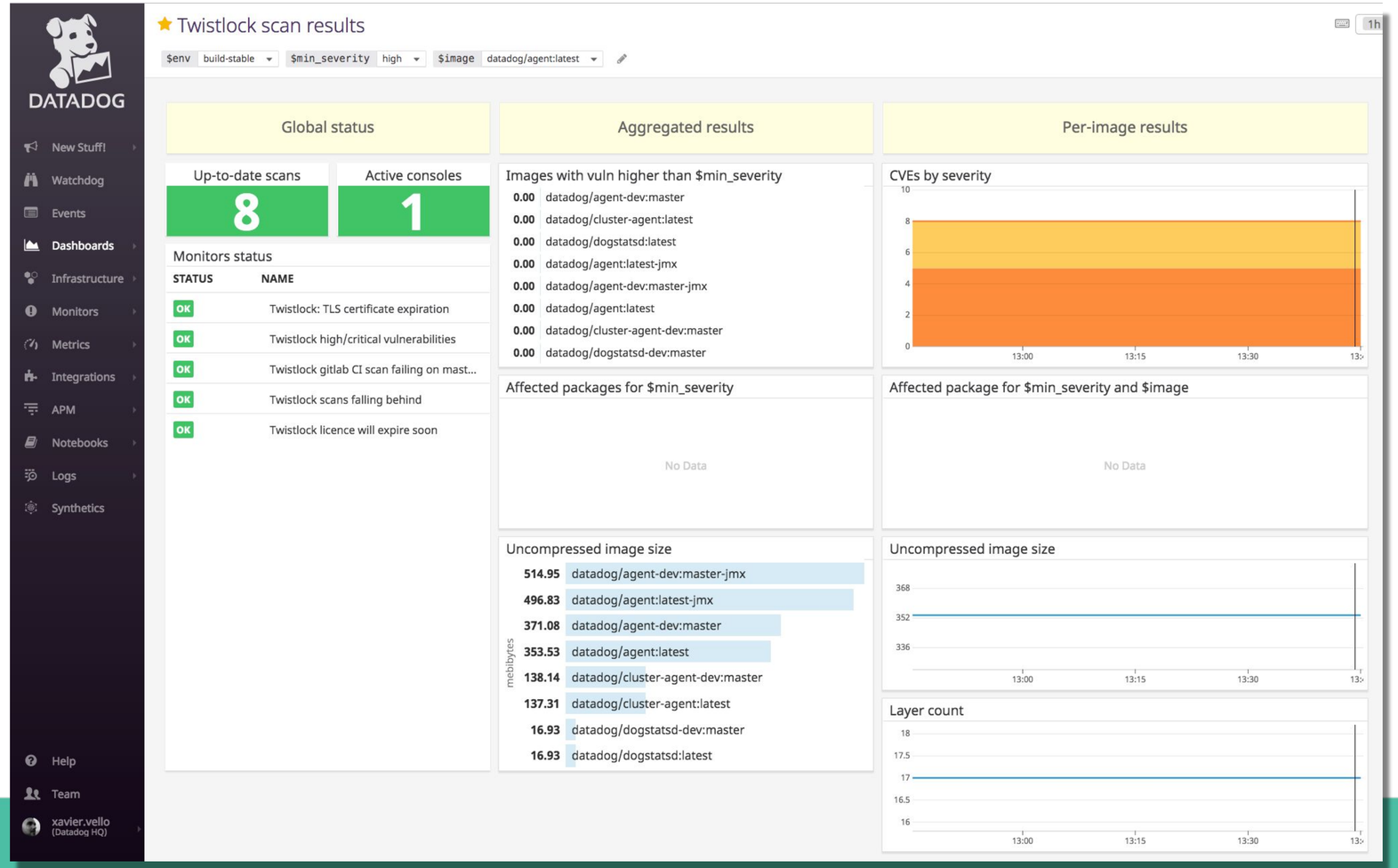


Recovered: Twistlock high/critical vulnerabilities on scanned_image:datadog/agent-dev:master,env:build-stable (4 kB)



Recovered: Twistlock high/critical vulnerabilities on env:build-stable,scanned_image:datadog/cluster-agent:latest (4 kB)





docker con 18 EUROPE

Takeaways

- Run several scanners
- Both master and latest
- Triage results as early as possible
- Investigate possible false positives

Thank you!
Questions?

xavier@xvello.net