Checkmarx

The world runs on code. We secure it.

KICS

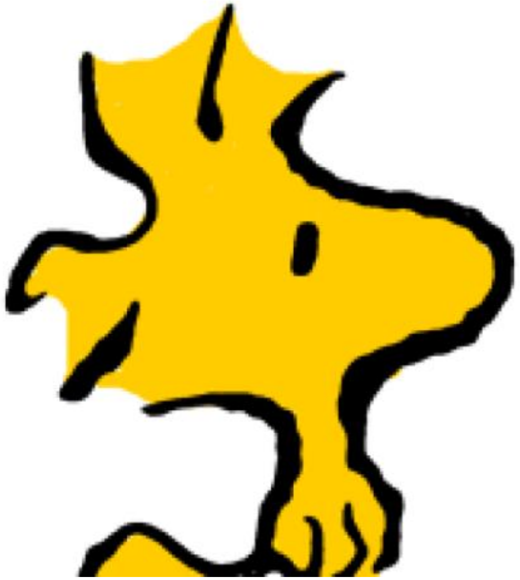
Community Meeting

2022.09.08

kics. by Checkmarx

Meet the KICS team

KICS 1.5 contributors (2+ commits)

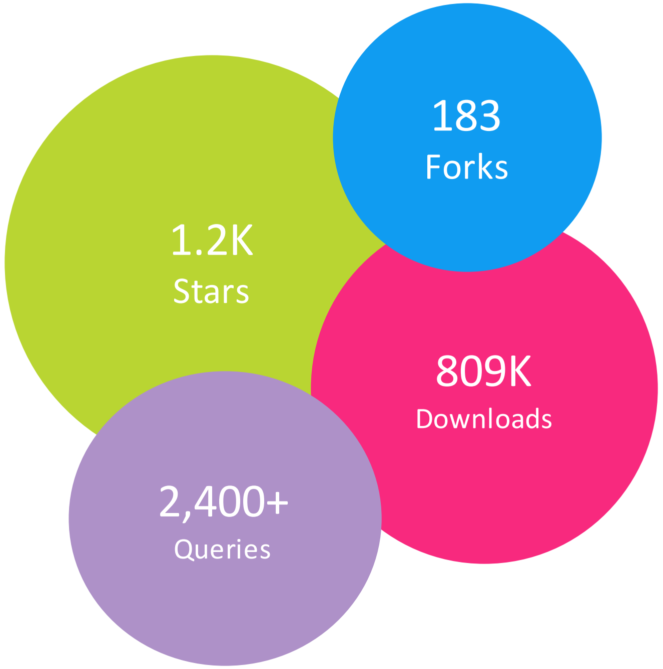


Community meetings

- **Bi-weekly meeting of the community & the KICS team.**
- **Meeting in mid sprint to:**
  - **Conclude the previous sprint & release**
  - **Talk about upcoming release & following sprint**
  - **Hear you, the community, on what interests you & what do you want to do / help with.**

KICS 1.5 contributors: @rndmh3ro @Churro @jplanckeel @AlexEndris @liorj-orca @lipeavelar @roi-orca @LupovichRan @ramprasathasokan @nv35 @konstruktoid @jaevans @roock @tspearconquest @jycamier @floh96 @rams3sh @gafnit-lightspin

KICS Community Updates



183
Forks

1.2K
Stars

809K
Downloads

2,400+
Queries

KICS 1.5.15 was released

KICS Github Action – updated to KICS 1.5.15

Community PR Merged (for KICS 1.6)

- None

Community PR Pending (for later)

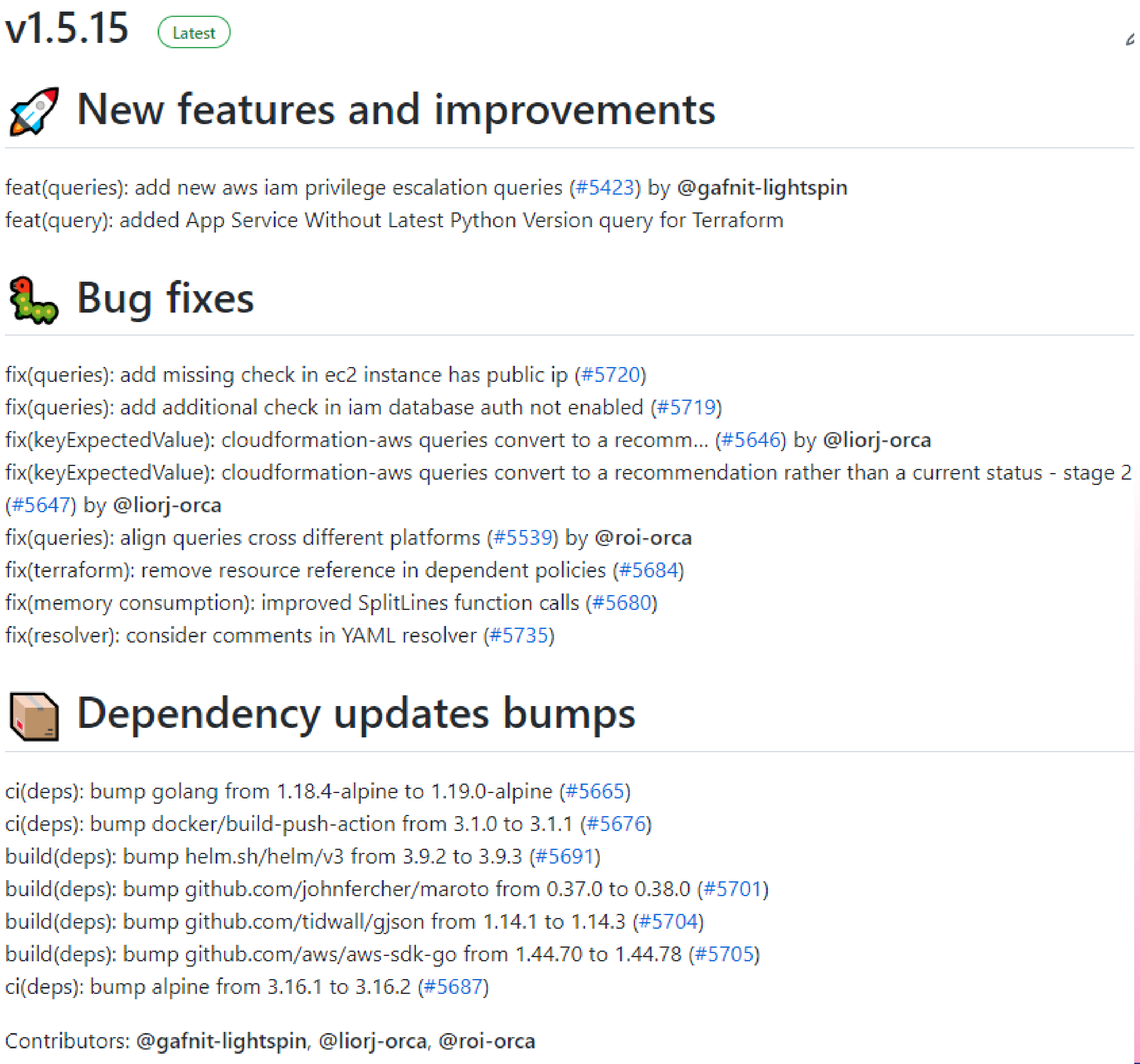
- change to use working directory when looking for `kics.config` #5319 - @lipeavelar
- add --ci flag to gitlab examples #5682 - @sluetze

Release

1.5.15 - 2022.08.31

- **Highlights**

- Added AWS IAM Privilege Escalation queries
- Added new Terraform query 'App Service Without Latest Python Version'
- Added comments support in YAML resolver
- Improved "Expected Value" in CloudFormation queries
- Queries aligned cross different platforms
- Added missing checks in several queries



v1.5.15 Latest

🚀 New features and improvements

feat(queries): add new aws iam privilege escalation queries (#5423) by **@gafnit-lightspin**
feat(query): added App Service Without Latest Python Version query for Terraform

🐛 Bug fixes

fix(queries): add missing check in ec2 instance has public ip (#5720)
fix(queries): add additional check in iam database auth not enabled (#5719)
fix(keyExpectedValue): cloudformation-aws queries convert to a recomm... (#5646) by **@liorj-orca**
fix(keyExpectedValue): cloudformation-aws queries convert to a recommendation rather than a current status - stage 2 (#5647) by **@liorj-orca**
fix(queries): align queries cross different platforms (#5539) by **@roi-orca**
fix(terraform): remove resource reference in dependent policies (#5684)
fix(memory consumption): improved SplitLines function calls (#5680)
fix(resolver): consider comments in YAML resolver (#5735)

📦 Dependency updates bumps

ci(deps): bump golang from 1.18.4-alpine to 1.19.0-alpine (#5665)
ci(deps): bump docker/build-push-action from 3.1.0 to 3.1.1 (#5676)
build(deps): bump helm.sh/helm/v3 from 3.9.2 to 3.9.3 (#5691)
build(deps): bump github.com/johnfercher/maroto from 0.37.0 to 0.38.0 (#5701)
build(deps): bump github.com/tidwall/gjson from 1.14.1 to 1.14.3 (#5704)
build(deps): bump github.com/aws/aws-sdk-go from 1.44.70 to 1.44.78 (#5705)
ci(deps): bump alpine from 3.16.1 to 3.16.2 (#5687)

Contributors: **@gafnit-lightspin**, **@liorj-orca**, **@roi-orca**

1.6 Release Plans

Feature Name	Due Date	Actual
K8S API Support – dynamic cluster scanning	Aug 2022	In Code Review
Support Pulumi (YAML only)	Aug 2022	Merged
Support Crossplane	Aug 2022	Merged
Support Serverless Framework	Aug 2022	In Code Review
Support Knative	Aug 2022	Merged
KICS Integration in Codefresh’s ArgoHub	Aug 2022	Under Approval

Planned releases:

- **1.6.0**
  - 14 September, 2022
- **1.6.1**
  - 28 September, 2022

Checkmarx

1.6.1 Release Plans

Feature Name	Due Date	Actual
BOM Support AWS RDS	Sep 2022	In investigation
BOM Support – AWS DynamoDB	Sep 2022	In investigation
BOM Support – AWS Aurora	Sep 2022	In investigation

Planned releases:

- **1.6.0**
  - 14 September, 2022
- **1.6.1**
  - 28 September, 2022

HacktoberFest Plans

KICS Auto-remediation feature: Add more queries and platforms to this feature (currently only for Terraform)

Extra queries for platforms added in 1.6: crossplane, pulumi, knative and serverless

Other, TBA

What is keeping us busy...

Terraformer

Change incorporation approach

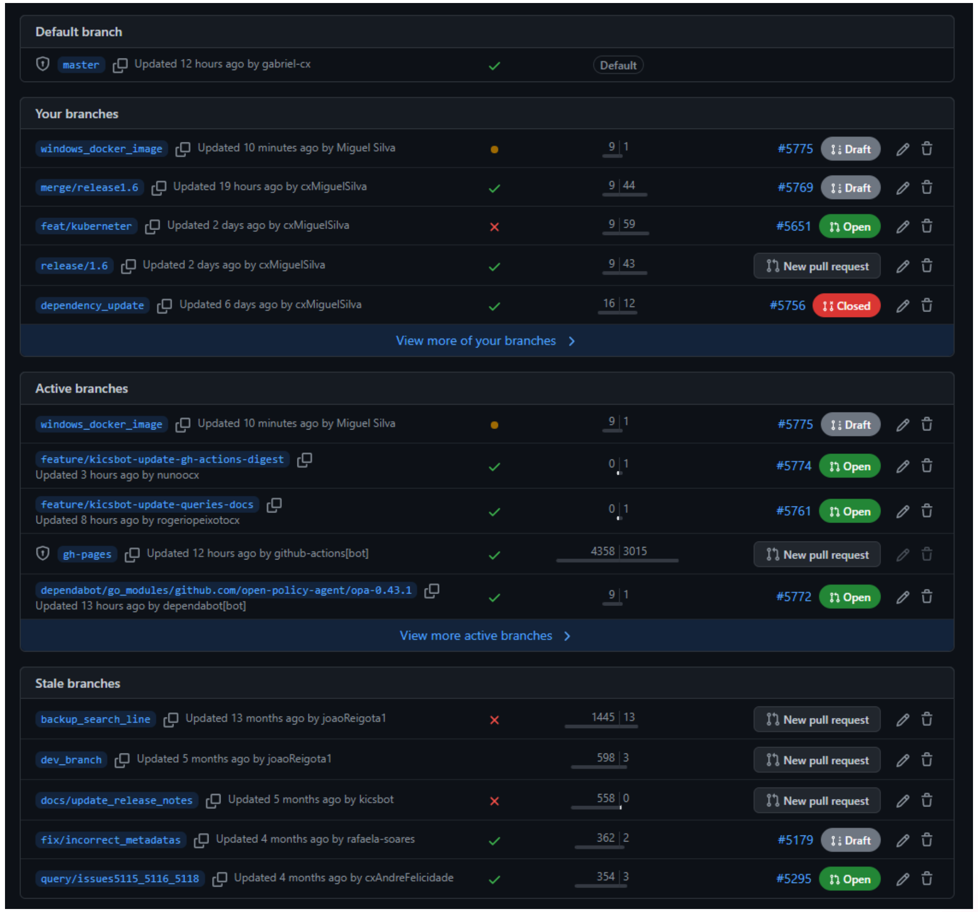
KICS now uses Terraformer as binary instead of importing It as a package. The change reduces the number of packages imported to the project (direct and indirectly) reducing also the risk of possible vulnerabilities in imported packages. As a result of this change the time to build the docker image was reduced.

Use

The use of the Terraformer feature in KICS did not change. Only the documentation was updated to go accordingly to the latest Terraformer version.

Branch CleanUp

All the open branches that were not in use were closed and deleted.



Default branch

master	Updated 12 hours ago by gabriel-cx	✓	Default	

Your branches

windows_docker_image	Updated 10 minutes ago by Miguel Silva	●	9 | 1	#5775 Draft
merge/release1.6	Updated 19 hours ago by cxMiguelSilva	✓	9 | 44	#5769 Draft
feat/kuberneter	Updated 2 days ago by cxMiguelSilva	✗	9 | 59	#5651 Open
release/1.6	Updated 2 days ago by cxMiguelSilva	✓	9 | 43	New pull request
dependency_update	Updated 6 days ago by cxMiguelSilva	✓	16 | 12	#5756 Closed

View more of your branches >

Active branches

windows_docker_image	Updated 10 minutes ago by Miguel Silva	●	9 | 1	#5775 Draft
feature/kicsbot-update-gh-actions-digest	Updated 3 hours ago by nunoocx	✓	0 | 1	#5774 Open
feature/kicsbot-update-queries-docs	Updated 8 hours ago by rogeriopeixotocx	✓	0 | 1	#5761 Open
gh-pages	Updated 12 hours ago by github-actions[bot]	✓	4358 | 3015	New pull request
dependabot/go_modules/github.com/open-policy-agent/opa-0.43.1	Updated 13 hours ago by dependabot[bot]	✓	9 | 1	#5772 Open

View more active branches >

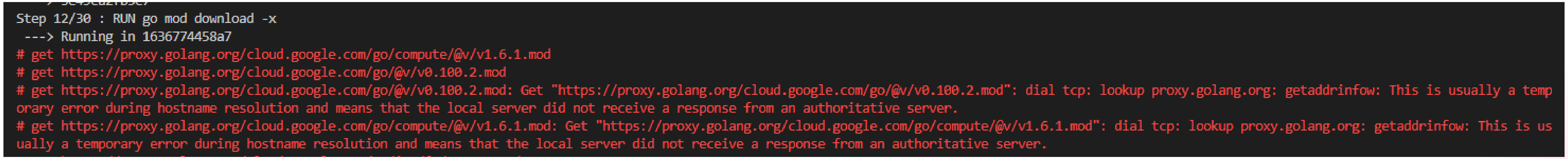
Stale branches

backup_search_line	Updated 13 months ago by joaoReigota1	✗	1445 | 13	New pull request
dev_branch	Updated 5 months ago by joaoReigota1		598 | 3	New pull request
docs/update_release_notes	Updated 5 months ago by kicsbot	✗	558 | 0	New pull request
fix/incorrect_metadatas	Updated 4 months ago by rafaela-soares	✓	362 | 2	#5179 Draft
query/issues5115_5116_5118	Updated 4 months ago by cxAndreFelicidade	✓	354 | 3	#5295 Open

WIP - Windows Docker Image

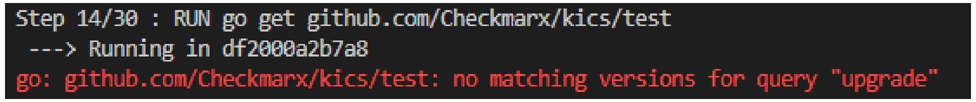
Some of the problems we have encountered in Windows Image creation:

Network Error when using VPN



```
Step 12/30 : RUN go mod download -x
 ---> Running in 1636774458a7
# get https://proxy.golang.org/cloud.google.com/go/compute/@v/v1.6.1.mod
# get https://proxy.golang.org/cloud.google.com/go/@v/v0.100.2.mod
# get https://proxy.golang.org/cloud.google.com/go/@v/v0.100.2.mod: Get "https://proxy.golang.org/cloud.google.com/go/@v/v0.100.2.mod": dial tcp: lookup proxy.golang.org: getaddrinfow: This is usually a temp
orary error during hostname resolution and means that the local server did not receive a response from an authoritative server.
# get https://proxy.golang.org/cloud.google.com/go/compute/@v/v1.6.1.mod: Get "https://proxy.golang.org/cloud.google.com/go/compute/@v/v1.6.1.mod": dial tcp: lookup proxy.golang.org: getaddrinfow: This is us
ually a temporary error during hostname resolution and means that the local server did not receive a response from an authoritative server.
```

Go Get Not working for private package during docker build



```
Step 14/30 : RUN go get github.com/Checkmarx/kics/test
 ---> Running in df2000a2b7a8
go: github.com/Checkmarx/kics/test: no matching versions for query "upgrade"
```

For community contribution:

#5775

WIP - Code Coverage

Currently, 77% of our code is covered by tests.
Our goal is to have, at least, 80-85% of code coverage in the next sprints.

For community contribution:
#5744

Research- GitHub Workflow Scanning

We are analyzing the possibility of scanning GitHub Workflows to detect security vulnerabilities.

Some vulnerabilities examples:

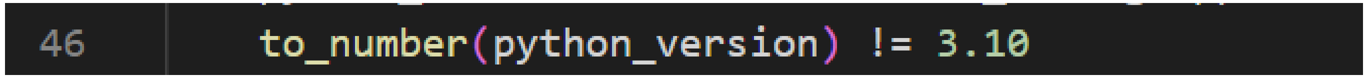
- **Code Execution via Unsafe User Inputs**
- **Exploiting pull_request_target**

Research- Dynamic way of checking tools latest versions

Currently, in our queries, we check if the used tools version is stable or not by comparing it with a 'static' value. That value is defined by us when we develop the query.
If a new version is released, of that same tool, we need to update the query by writing the new version tag.

We want to have a more dynamic process to check the latest tools versions.

Example of the current implementation:



```
    to_number(python_version) != 3.10
```

Hearing from the Community

- **Open floor for all participants**

kics.

by Checkmarx