Checkmarx

The world runs on code. We secure it.

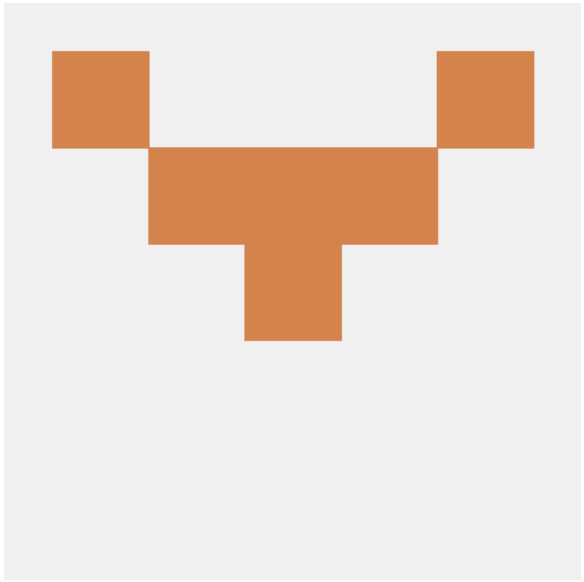
KICS

Community Meeting

2022.11.03

Meet the KICS team

KICS contributors (2+ commits)



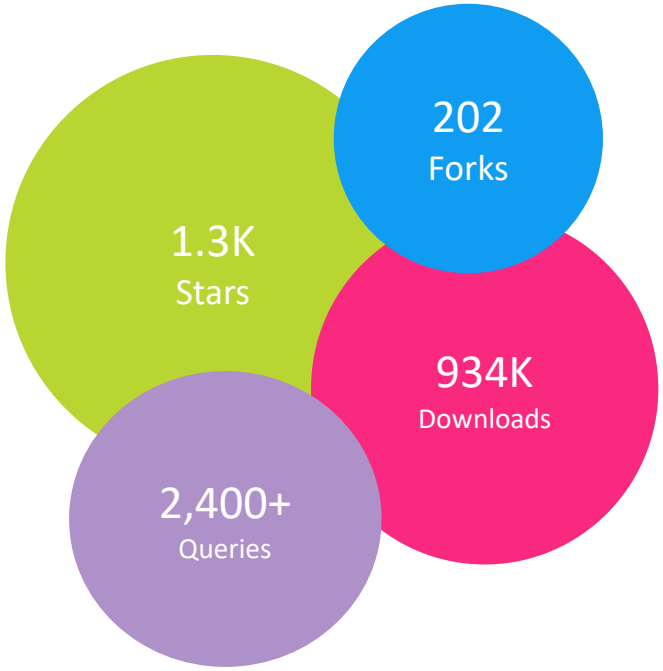
Community meetings

- **Monthly meeting of the community & the KICS team.**
- **Meeting 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 1.6 contributors:
@sluetze @tomk-orca @liorj-orca @konstruktoid @VladMasarik @jycamier @Churro @patrickpichler @JoaoDanielRufino

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 – 2022-11-03



KICS 1.6.2 and 1.6.3 were released

Community PR Merged (for KICS 1.6.4)

+ fix(query): fix queries expected value #5970 - @liorj-orca

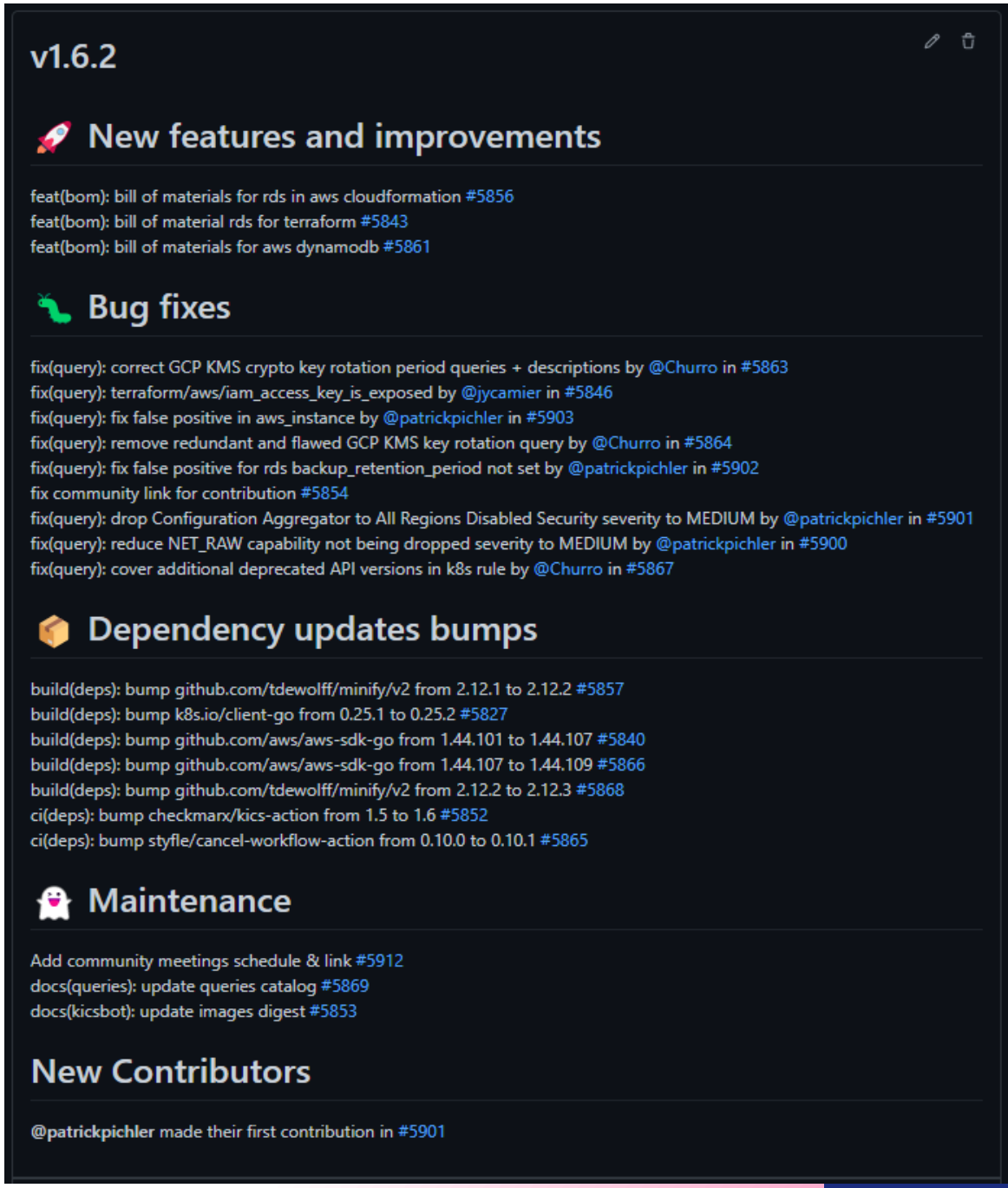
Community PR Pending (for later version)

+ change to use working directory when looking for `kics.config` #5319 - @lipeavelar
+ fix(query): S3 Bucket Without Restriction Of Public Bucket Security Query False Positive Result #5911 - @JoaoDanielRufino
+ fix: changing directory name of viewer_protocol_policy_allows_http #5981 - @jycamier

Release

1.6.2 - 2022.10.13

- **Highlights**
- New BOM
- Bug fixes



v1.6.2

New features and improvements

feat(bom): bill of materials for rds in aws cloudformation #5856
feat(bom): bill of material rds for terraform #5843
feat(bom): bill of materials for aws dynamodb #5861

Bug fixes

fix(query): correct GCP KMS crypto key rotation period queries + descriptions by @Churro in #5863
fix(query): terraform/aws/iam_access_key_is_exposed by @jycamier in #5846
fix(query): fix false positive in aws_instance by @patrickpichler in #5903
fix(query): remove redundant and flawed GCP KMS key rotation query by @Churro in #5864
fix(query): fix false positive for rds backup_retention_period not set by @patrickpichler in #5902
fix community link for contribution #5854
fix(query): drop Configuration Aggregator to All Regions Disabled Security severity to MEDIUM by @patrickpichler in #5901
fix(query): reduce NET_RAW capability not being dropped severity to MEDIUM by @patrickpichler in #5900
fix(query): cover additional deprecated API versions in k8s rule by @Churro in #5867

Dependency updates bumps

build(deps): bump github.com/tdewolff/minify/v2 from 2.12.1 to 2.12.2 #5857
build(deps): bump k8s.io/client-go from 0.25.1 to 0.25.2 #5827
build(deps): bump github.com/aws/aws-sdk-go from 1.44.101 to 1.44.107 #5840
build(deps): bump github.com/aws/aws-sdk-go from 1.44.107 to 1.44.109 #5866
build(deps): bump github.com/tdewolff/minify/v2 from 2.12.2 to 2.12.3 #5868
ci(deps): bump checkmarx/kics-action from 1.5 to 1.6 #5852
ci(deps): bump styfle/cancel-workflow-action from 0.10.0 to 0.10.1 #5865

Maintenance

Add community meetings schedule & link #5912
docs(queries): update queries catalog #5869
docs(kicsbot): update images digest #5853

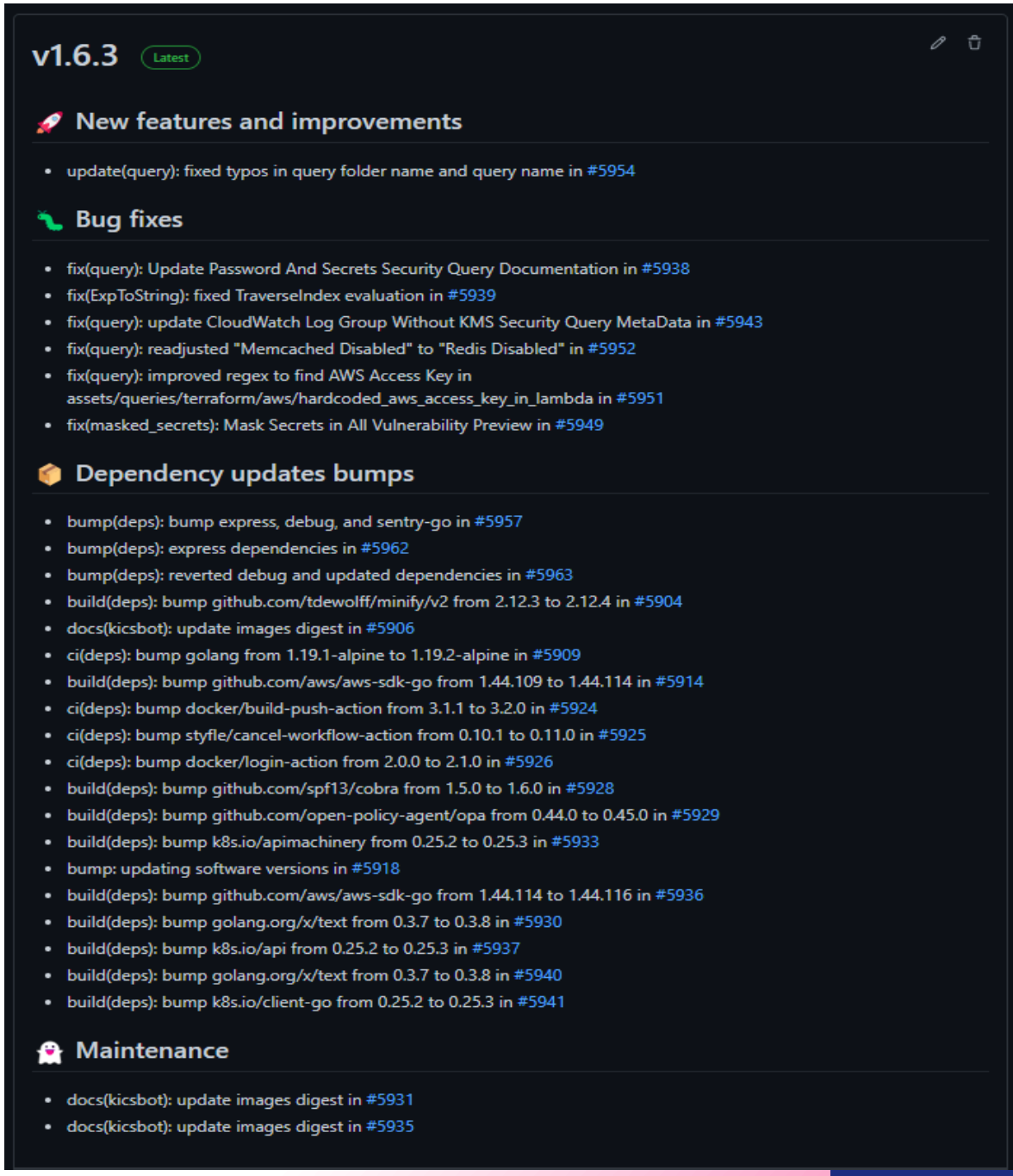
New Contributors

@patrickpichler made their first contribution in #5901

Release

1.6.3 - 2022.10.26

- **Highlights**
- Bug fixes



v1.6.3 Latest

New features and improvements

- update(query): fixed typos in query folder name and query name in #5954

Bug fixes

- fix(query): Update Password And Secrets Security Query Documentation in #5938
- fix(ExpToString): fixed TraverseIndex evaluation in #5939
- fix(query): update CloudWatch Log Group Without KMS Security Query MetaData in #5943
- fix(query): readjusted "Memcached Disabled" to "Redis Disabled" in #5952
- fix(query): improved regex to find AWS Access Key in assets/queries/terraform/aws/hardcoded_aws_access_key_in_lambda in #5951
- fix(masked_secrets): Mask Secrets in All Vulnerability Preview in #5949

Dependency updates bumps

- bump(deps): bump express, debug, and sentry-go in #5957
- bump(deps): express dependencies in #5962
- bump(deps): reverted debug and updated dependencies in #5963
- build(deps): bump github.com/tdewolff/minify/v2 from 2.12.3 to 2.12.4 in #5904
- docs(kicsbot): update images digest in #5906
- ci(deps): bump golang from 1.19.1-alpine to 1.19.2-alpine in #5909
- build(deps): bump github.com/aws/aws-sdk-go from 1.44.109 to 1.44.114 in #5914
- ci(deps): bump docker/build-push-action from 3.1.1 to 3.2.0 in #5924
- ci(deps): bump styfle/cancel-workflow-action from 0.10.1 to 0.11.0 in #5925
- ci(deps): bump docker/login-action from 2.0.0 to 2.1.0 in #5926
- build(deps): bump github.com/spf13/cobra from 1.5.0 to 1.6.0 in #5928
- build(deps): bump github.com/open-policy-agent/opa from 0.44.0 to 0.45.0 in #5929
- build(deps): bump k8s.io/apimachinery from 0.25.2 to 0.25.3 in #5933
- bump: updating software versions in #5918
- build(deps): bump github.com/aws/aws-sdk-go from 1.44.114 to 1.44.116 in #5936
- build(deps): bump golang.org/x/text from 0.3.7 to 0.3.8 in #5930
- build(deps): bump k8s.io/api from 0.25.2 to 0.25.3 in #5937
- build(deps): bump golang.org/x/text from 0.3.7 to 0.3.8 in #5940
- build(deps): bump k8s.io/client-go from 0.25.2 to 0.25.3 in #5941

Maintenance

- docs(kicsbot): update images digest in #5931
- docs(kicsbot): update images digest in #5935

1.6.4 Release Plans

Feature Name	Due Date	Actual
OpenSSL vulnerable version support	Nov 2022	Done
BOM Support: Amazon Kinesis, Cassandra & Hadoop	Nov 2022	In backlog

Planned releases:

- **1.6.4**
  - 09 November, 2022

What is keeping us busy...

OpenSSL Vulnerable Versions

> OpenSSL versions from 3.0.0 to 3.0.5* are affected by a critical vulnerability

(*) version 3.0.6 is not available in the OpenSSL downloads

CVE-2022-3786 (OpenSSL advisory) [HIGH severity] 01 November 2022:

A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Reported by Viktor Dukhovni.

- Fixed in OpenSSL 3.0.7 (git commit) (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6)

CVE-2022-3602 (OpenSSL advisory) [HIGH severity] 01 November 2022:

A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Reported by Polar Bear.

- Fixed in OpenSSL 3.0.7 (git commit) (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6)

OpenSSL Vulnerable Versions

> KICS v.1.6.4 will have a new query "Vulnerable OpenSSL Versions" that can be used in previous versions as a custom query

[KICS version < 1.5.14]

These KICS versions will only be able to detect OpenSSL vulnerable versions that are part of the URL

```
FROM ubuntu
RUN wget -O- https://www.openssl.org/source/openssl-3.0.0.tar.gz
```

[KICS version >= 1.5.14 & KICS version < 1.6.4]

These KICS versions can detect OpenSSL vulnerable versions that are part of the URL or if it is defined by using the ARG command

```
FROM ubuntu

ARG OPENSSL_SRC=https://www.openssl.org/source/openssl-3.0.4.tar.gz

RUN curl ${OPENSSL_SRC}
```

OpenSSL Vulnerable Versions

[KICS version >= 1.6.4]

These KICS versions can detect OpenSSL vulnerable versions that are part of the URL or if it is defined by using the ARG/ENV

```
FROM ubuntu

ENV OPENSSL3_URL=https://www.openssl.org/source/openssl-3.0.2.tar.gz

RUN apk update \
    && apk upgrade \
    && apk add make gcc

RUN yum -y install \
    && yum clean all \
    && wget $OPENSSL3_URL
```

Custom queries support for Remediation command

new --queries flag in remediation command

vs.

stocking the absolute query path in the results.json

Should KICS override query metadata?

Capacity to override the metadatas of a query #5849

Open jycamier opened this issue on 28 Sep · 8 comments

jycamier commented on 28 Sep • edited Contributor

Is your feature request related to a problem? Please describe.

As a final user of KICS, I would like to override the `metadata.json` file of a query :

- to set my own documentation in `descriptionUrl`
- to set my own severity level on a query

Describe the solution you'd like

I would like the possibility to add in my queries a new query with a single `metadata.json` file referring to an existing query ID.

Describe alternatives you've considered

- ignore the existing query
- copy /past this one in my own query directory
- change the query ID

Be able to override severity level #5960

Open LvffY opened this issue 11 days ago · 0 comments

LvffY commented 11 days ago

Is your feature request related to a problem? Please describe.

For now, we can only exclude queries based on our needs. It could be great to have a way to override the severity of each feature for multiple reasons :

- In case of high severity issue that can't be fixed, just excluding the issue could lead to just ignoring the problems
- In some context, people can think that the severity used by kics is too low and would like to increase the severity for some rules

Thanks to that, the report provided by kics could be more usefule and accurante than they already are.

Describe the solution you'd like

I think that this could be added in the configuration files. For exemple in an **overrides** section. For example, in a YAML format, this could lead to this kind of YAML file :

```
overrides:
  - rule: ID_OF_THE_RULE1
    severity: High
  - rule: ID_OF_THE_RULE2
    severity: Info
...
```

Describe alternatives you've considered

For now, we can only completely excludes rules or disable them file by file, line by line or block by block. In case of a general rule, this could be error prone and quite complicated.

Hearing from the Community

KICS.

by Checkmarx