Filters Clear All Filters

Looking for Bugs, Vulnerabilities, or Code Smells? If your team prefers working with these types, change it in the **settings**

Language

Search for languages...

Docker 1

1 shown

Software quality

Security 1

Reliability 0

Maintainability 0

Security Hotspots

Show Security Hotspots Only 0

Severity

Blocker 1

High 0

Medium 0

Low 0

Credentials should not be hard-coded

Rule ID: **docker:S6437** Analysis scope: **main sources** Rule repo: **Sonar (Docker)** Effort: **1h**

cwe +

Software qualities impacted

Security Blocker

Code attribute

Responsibility | Trustworthy

Why is this an issue? How can I fix it? More info

Secret leaks often occur when a sensitive piece of authentication data is stored with the source code of an application. Considering the source code is intended to be deployed across multiple assets, including source code repositories or application hosting servers, the secrets might get exposed to an unintended audience.

In most cases, trust boundaries are violated when a secret is exposed in a source code repository or an uncontrolled deployment environment. Unintended people who don't need to know the secret might get access to it. They might then be able to use it to gain unwanted access to associated services or resources.

The trust issue can be more or less severe depending on the people's role and entitlement.

In Dockerfiles, hard-coded secrets and secrets passed through as variables or created at build-time will cause security risks. The secret information can be exposed either via the container environment, the image metadata, or the build environment logs.

What is the potential impact?

The consequences vary greatly depending on the situation and the secret-exposed audience. Still, two main scenarios should be considered.

Financial loss

Financial losses can occur when a secret is used to access a paid third-party-provided service and is disclosed as part of the source code of client applications. Having the secret, each user of the application will be able to use it without limit to use the third party service to their own need, including in a way that was not expected.

This additional use of the secret will lead to added costs with the service provider.

Moreover, when rate or volume limiting is set up on the provider side, this additional use can prevent the regular operation of the affected application. This might result in a partial denial of service for all the application's users.