|  |  |
| --- | --- |
| **SCR-1.2: Dockerfile Misconfiguration: Default User Privilege** | **No. of Findings: 1** |
| **Description**  The Dockerfile does not specify a USER, so it defaults to running with a root user.   |  |  |  |  | | --- | --- | --- | --- | | **Source location and affected line number (parent)** | **Line number variable/method affected (child)** | **Risk Rating** | **Variable/method affected** | | Dockerfile/Dockerfile | 1 | High | FROM python:3.7-alpine as builder RUN apk --update add bash nano g++ COPY . /vampi | | |
| **Implications**  When a Dockerfile does not specify a USER, Docker containers run with super user privileges by default. These super user privileges are propagated to the code running inside the container, which is usually more permission than necessary. Running the Docker container with super user privileges broadens the attack surface which might enable attackers to perform more serious forms of exploitation. | |
| **Recommendations**  It is good practice to run your containers as a non-root user when possible. To modify a docker container to use a non-root user, the Dockerfile needs to specify a different user, such as: RUN useradd myLowPrivilegeUser USER myLowPrivilegeUser | |
| **Management Comments** | |
| **Follow-up** | |