# CVE Detail – CVE-2022-36109

Moby is an open-source project created by Docker to enable software containerization. A bug was found in Moby (Docker Engine) where supplementary groups are not set up properly. If an attacker has direct access to a container and manipulates their supplementary group access, they may be able to use supplementary group access to bypass primary group restrictions in some cases, potentially gaining access to sensitive information or gaining the ability to execute code in that container. This bug is fixed in Moby (Docker Engine) 20.10.18. Running containers should be stopped and restarted for the permissions to be fixed. For users unable to upgrade, this problem can be worked around by not using the `"USER $USERNAME"` Dockerfile instruction. Instead by calling `ENTRYPOINT ["su", "-", "user"]` the supplementary groups will be set up properly.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.06072

## CVSS Scoring

CVSS v3.1 Score: 5.3

Severity: MEDIUM

## Mapped CWE(s)

* CWE-863: Incorrect Authorization

## Affected Products

* cpe:2.3:a:mobyproject:moby:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:36:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:37:\*:\*:\*:\*:\*:\*:\*