# CWE Detail – CWE-538

## Description

The product places sensitive information into files or directories that are accessible to actors who are allowed to have access to the files, but not to the sensitive information.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2018-1999036: SSH password for private key stored in build log

## Related Attack Patterns (CAPEC)

* CAPEC-95

## Modes of Introduction

**•** Implementation: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

**•** Operation: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

## Common Consequences

**•** Impact: Read Files or Directories — Notes:

## Potential Mitigations

**•** Architecture and Design: Do not expose file and directory information to the user. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** N/A

## Notes

**•** Maintenance: Depending on usage, this could be a weakness or a category. Further study of all its children is needed, and the entire sub-tree may need to be clarified. The current organization is based primarily on the exposure of sensitive information as a consequence, instead of as a primary weakness.

**•** Maintenance: There is a close relationship with CWE-552, which is more focused on weaknesses. As a result, it may be more appropriate to convert CWE-538 to a category.