# CWE Detail – CWE-922

## Description

The product stores sensitive information without properly limiting read or write access by unauthorized actors.

## Extended Description

If read access is not properly restricted, then attackers can steal the sensitive information. If write access is not properly restricted, then attackers can modify and possibly delete the data, causing incorrect results and possibly a denial of service.

## Threat-Mapped Scoring

Score: 3.1

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2009-2272: password and username stored in cleartext in a cookie

## Modes of Introduction

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

**•** Implementation: N/A

**•** System Configuration: N/A

## Common Consequences

**•** Impact: Read Application Data, Read Files or Directories — Notes: Attackers can read sensitive information by accessing the unrestricted storage mechanism.

**•** Impact: Modify Application Data, Modify Files or Directories — Notes: Attackers can overwrite sensitive information by accessing the unrestricted storage mechanism.

## Applicable Platforms

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

## Notes

**•** Relationship: There is an overlapping relationship between insecure storage of sensitive information (CWE-922) and missing encryption of sensitive information (CWE-311). Encryption is often used to prevent an attacker from reading the sensitive data. However, encryption does not prevent the attacker from erasing or overwriting the data. While data tampering would be visible upon inspection, the integrity and availability of the data is compromised prior to the audit.

**•** Maintenance: This is a high-level entry that includes children from various parts of the CWE research view (CWE-1000). Currently, most of the information is in these child entries. This entry will be made more comprehensive in later CWE versions.