# CWE Detail – CWE-276

## Description

During installation, installed file permissions are set to allow anyone to modify those files.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2005-1941: Executables installed world-writable.

**•** CVE-2002-1713: Home directories installed world-readable.

**•** CVE-2001-1550: World-writable log files allow information loss; world-readable file has cleartext passwords.

**•** CVE-2002-1711: World-readable directory.

**•** CVE-2002-1844: Windows product uses insecure permissions when installing on Solaris (genesis: port error).

**•** CVE-2001-0497: Insecure permissions for a shared secret key file. Overlaps cryptographic problem.

**•** CVE-1999-0426: Default permissions of a device allow IP spoofing.

## Related Attack Patterns (CAPEC)

* CAPEC-1
* CAPEC-127
* CAPEC-81

## Attack TTPs

**•** T1083: File and Directory Discovery (Tactics: discovery)

**•** T1574.010: Services File Permissions Weakness (Tactics: persistence, privilege-escalation, defense-evasion)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Installation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data, Modify Application Data — Notes:

## Potential Mitigations

**•** Architecture and Design: The architecture needs to access and modification attributes for files to only those users who actually require those actions. (Effectiveness: N/A)

**•** Architecture and Design: Compartmentalize the system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area. Ensure that appropriate compartmentalization is built into the system design, and the compartmentalization allows for and reinforces privilege separation functionality. Architects and designers should rely on the principle of least privilege to decide the appropriate time to use privileges and the time to drop privileges. (Effectiveness: N/A)

## Applicable Platforms

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