# CWE Detail – CWE-689

## Description

The product, while copying or cloning a resource, does not set the resource's permissions or access control until the copy is complete, leaving the resource exposed to other spheres while the copy is taking place.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2002-0760: Archive extractor decompresses files with world-readable permissions, then later sets permissions to what the archive specified.

**•** CVE-2005-2174: Product inserts a new object into database before setting the object's permissions, introducing a race condition.

**•** CVE-2006-5214: Error file has weak permissions before a chmod is performed.

**•** CVE-2005-2475: Archive permissions issue using hard link.

**•** CVE-2003-0265: Database product creates files world-writable before initializing the setuid bits, leading to modification of executables.

## Related Attack Patterns (CAPEC)

* CAPEC-26
* CAPEC-27

## Modes of Introduction

**•** Implementation: Common examples occur in file archive extraction, in which the product begins the extraction with insecure default permissions, then only sets the final permissions (as specified in the archive) once the copy is complete. The larger the archive, the larger the timing window for the race condition. This weakness has also occurred in some operating system utilities that perform copies of deeply nested directories containing a large number of files. This weakness can occur in any type of functionality that involves copying objects or resources in a multi-user environment, including at the application level. For example, a document management system might allow a user to copy a private document, but if it does not set the new copy to be private as soon as the copy begins, then other users might be able to view the document while the copy is still taking place.

## Common Consequences

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

## Applicable Platforms

**•** C (Class: None, Prevalence: Undetermined)

**•** Perl (Class: None, Prevalence: Undetermined)

## Notes

**•** Research Gap: Under-studied. It seems likely that this weakness could occur in any situation in which a complex or large copy operation occurs, when the resource can be made available to other spheres as soon as it is created, but before its initialization is complete.