# CWE Detail – CWE-214

## Description

A process is invoked with sensitive command-line arguments, environment variables, or other elements that can be seen by other processes on the operating system.

## Extended Description

Many operating systems allow a user to list information about processes that are owned by other users. Other users could see information such as command line arguments or environment variable settings. When this data contains sensitive information such as credentials, it might allow other users to launch an attack against the product or related resources.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2005-1387: password passed on command line

**•** CVE-2005-2291: password passed on command line

**•** CVE-2001-1565: username/password on command line allows local users to view via "ps" or other process listing programs

**•** CVE-2004-1948: Username/password on command line allows local users to view via "ps" or other process listing programs.

**•** CVE-1999-1270: PGP passphrase provided as command line argument.

**•** CVE-2004-1058: Kernel race condition allows reading of environment variables of a process that is still spawning.

**•** CVE-2021-32638: Code analysis product passes access tokens as a command-line parameter or through an environment variable, making them visible to other processes via the ps command.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

**•** Operation: N/A

## Common Consequences

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

## Applicable Platforms

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

## Demonstrative Examples

**•** If the property is defined on the command line when the program is invoked (using the -D... syntax), the password may be displayed in the OS process list.

## Notes

**•** Research Gap: Under-studied, especially environment variables.