# CWE Detail – CWE-589

## Description

The product uses an API function that does not exist on all versions of the target platform. This could cause portability problems or inconsistencies that allow denial of service or other consequences.

## Extended Description

Some functions that offer security features supported by the OS are not available on all versions of the OS in common use. Likewise, functions are often deprecated or made obsolete for security reasons and should not be used.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-96

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Quality Degradation — Notes:

## Potential Mitigations

**•** Implementation: Always test your code on any platform on which it is targeted to run on. (Effectiveness: N/A)

**•** Testing: Test your code on the newest and oldest platform on which it is targeted to run on. (Effectiveness: N/A)

**•** Testing: Develop a system to test for API functions that are not portable. (Effectiveness: N/A)