# CWE Detail – CWE-420

## Description

The product protects a primary channel, but it does not use the same level of protection for an alternate channel.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2020-8004: When the internal flash is protected by blocking access on the Data Bus (DBUS), it can still be indirectly accessed through the Instruction Bus (IBUS).

**•** CVE-2002-0567: DB server assumes that local clients have performed authentication, allowing attacker to directly connect to a process to load libraries and execute commands; a socket interface also exists (another alternate channel), so attack can be remote.

**•** CVE-2002-1578: Product does not restrict access to underlying database, so attacker can bypass restrictions by directly querying the database.

**•** CVE-2003-1035: User can avoid lockouts by using an API instead of the GUI to conduct brute force password guessing.

**•** CVE-2002-1863: FTP service can not be disabled even when other access controls would require it.

**•** CVE-2002-0066: Windows named pipe created without authentication/access control, allowing configuration modification.

**•** CVE-2004-1461: Router management interface spawns a separate TCP connection after authentication, allowing hijacking by attacker coming from the same IP address.

## 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

**•** Operation: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Identify all alternate channels and use the same protection mechanisms that are used for the primary channels. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The bugged line of code is repeated in the Bad
 example above. The weakness arises from the fact that the
 SECURE\_ME register can be modified by writing to the
 shadow register COPY\_OF\_SECURE\_ME. The address of
 COPY\_OF\_SECURE\_ME should also be included in the check.
 That buggy line of code should instead be replaced as
 shown in the Good Code Snippet below.

## Notes

**•** Relationship: This can be primary to authentication errors, and resultant from unhandled error conditions.