# CWE Detail – CWE-1261

## Description

The hardware logic does not effectively handle when single-event upsets (SEUs) occur.

## Extended Description

Technology trends such as CMOS-transistor down-sizing, use of
 new materials, and system-on-chip architectures continue to increase the
 sensitivity of systems to soft errors. These errors are random, and
 their causes might be internal (e.g., interconnect coupling) or external
 (e.g., cosmic radiation). These soft errors are not permanent in nature
 and cause temporary bit flips known as single-event upsets (SEUs).
 SEUs are induced errors in circuits caused when charged particles lose
 energy by ionizing the medium through which they pass, leaving behind a
 wake of electron-hole pairs that cause temporary failures. If these
 failures occur in security-sensitive modules in a chip, it might
 compromise the security guarantees of the chip. For instance, these
 temporary failures could be bit flips that change the privilege of
 a regular user to root.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart, DoS: Instability, Gain Privileges or Assume Identity, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Implement triple-modular redundancy around security-sensitive modules. (Effectiveness: N/A)

**•** Architecture and Design: SEUs mostly affect SRAMs. For SRAMs storing security-critical data, implement Error-Correcting-Codes (ECC) and Address Interleaving. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Parity is error detecting but not error correcting.

**•** N/A