# CWE Detail – CWE-453

## Description

The product, by default, initializes an internal variable with an insecure or less secure value than is possible.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2022-36349: insecure default variable initialization in BIOS firmware for a hardware board allows DoS

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Application Data — Notes: An attacker could gain access to and modify sensitive data or system information.

## Potential Mitigations

**•** System Configuration: Disable or change default settings when they can be used to abuse the system. Since those default settings are shipped with the product they are likely to be known by a potential attacker who is familiar with the product. For instance, default credentials should be changed or the associated accounts should be disabled. (Effectiveness: N/A)

## Applicable Platforms

**•** PHP (Class: None, Prevalence: Sometimes)

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

## Demonstrative Examples

**•** Because the $authorized variable is never initialized, PHP will automatically set $authorized to any value included in the POST request if register\_globals is enabled. An attacker can send a POST request with an unexpected third value 'authorized' set to 'true' and gain authorized status without supplying valid credentials.

## Notes

**•** Maintenance: This overlaps other categories, probably should be split into separate items.