# CWE Detail – CWE-1188

## Description

The product initializes or sets a resource with a default that is intended to be changed by the administrator, but the default is not secure.

## Extended Description

Developers often choose default values that leave the product as open and easy to use as possible out-of-the-box, under the assumption that the administrator can (or should) change the default value. However, this ease-of-use comes at a cost when the default is insecure and the administrator does not change it.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

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

**•** CVE-2022-42467: A generic database browser interface has a default mode that exposes a web server to the network, allowing queries to the database.

## Related Attack Patterns (CAPEC)

* CAPEC-665

## Attack TTPs

**•** T1542.002: Component Firmware (Tactics: persistence, defense-evasion)

**•** T1556: Modify Authentication Process (Tactics: credential-access, defense-evasion, persistence)

**•** T1211: Exploitation for Defense Evasion (Tactics: defense-evasion)

## 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 entry improves organization of concepts under initialization. The typical CWE model is to cover "Missing" and "Incorrect" behaviors. Arguably, this entry could be named as "Incorrect" instead of "Insecure." This might be changed in the near future.