# CWE Detail – CWE-913

## Description

The product does not properly restrict reading from or writing to dynamically-managed code resources such as variables, objects, classes, attributes, functions, or executable instructions or statements.

## Extended Description

Many languages offer powerful features that allow the programmer to dynamically create or modify existing code, or resources used by code such as variables and objects. While these features can offer significant flexibility and reduce development time, they can be extremely dangerous if attackers can directly influence these code resources in unexpected ways.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2022-2054: Python compiler uses eval() to execute malicious strings as Python code.

**•** CVE-2018-1000613: Cryptography API uses unsafe reflection when deserializing a private key

**•** CVE-2015-8103: Deserialization issue in commonly-used Java library allows remote execution.

**•** CVE-2006-7079: Chain: extract used for register\_globals compatibility layer, enables path traversal (CWE-22)

**•** CVE-2012-2055: Source version control product allows modification of trusted key using mass assignment.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Execute Unauthorized Code or Commands — Notes:

**•** Impact: Varies by Context, Alter Execution Logic — Notes:

## Potential Mitigations

**•** Implementation: For any externally-influenced input, check the input against an allowlist of acceptable values. (Effectiveness: N/A)

**•** Implementation: Refactor the code so that it does not need to be dynamically managed. (Effectiveness: N/A)