# CWE Detail – CWE-1085

## Description

A function, method, procedure, etc. contains an excessive amount of code that has been  
 commented out within its body.

## Extended Description

This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities. While the interpretation of "excessive volume" may vary for each product or developer, CISQ recommends a default threshold of 2% of commented code.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Common Consequences

**•** Impact: Reduce Maintainability — Notes: