# CWE Detail – CWE-1125

## Description

The product has an attack surface whose quantitative
 measurement exceeds a desirable maximum.

## Extended Description

Originating from software security, an "attack surface" measure typically reflects the number of input points and output points that can be utilized by an untrusted party, i.e. a potential attacker. A larger attack surface provides more places to attack, and more opportunities for developers to introduce weaknesses. In some cases, this measure may reflect other aspects of quality besides security; e.g., a product with many inputs and outputs may require a large number of tests in order to improve code coverage.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified