



A Community-Developed List of Software Weakness Types


[Home](#)
[About](#)
[CWE List](#)
[Scoring
Search](#)
[Community](#)
[News](#)
Weakness ID: 200
Abstraction: Class

Structure: Simple

Status: Incomplete

Presentation Filter:

▼ Description

An information exposure is the intentional or unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information.

▼ Extended Description

The information either:

1. is regarded as sensitive within the product's own functionality, such as a private message; or
2. provides information about the product or its environment that could be useful in an attack but is normally not available to the attacker, such as the installation path of a product that is remotely accessible.

Many information exposures are resultant (e.g. PHP script error revealing the full path of the program), but they can also be primary (e.g. timing discrepancies in cryptography). There are many different types of problems that involve information exposures. Their severity can range widely depending on the type of information that is revealed.

▼ Alternate Terms

Information Leak:

This is a frequently used term, however the "leak" term has multiple uses within security. In some cases it deals with exposure of information, but in other cases (such as "memory leak") this deals with improper tracking of resources which can lead to exhaustion. As a result, CWE is actively avoiding usage of the "leak" term.

Information Disclosure:

This term is frequently used in vulnerability databases and other sources, however "disclosure" does not always have security implications. The phrase "information disclosure" is also used frequently in policies and legal documents, but do not refer to disclosure of security-relevant information.

▼ Relationships

The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.

- ▶ **Relevant to the view "Research Concepts" (CWE-1000)**
- ▶ **Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)**
- ▶ **Relevant to the view "Development Concepts" (CWE-699)**

▼ Modes Of Introduction

WIZ, Inc. EXHIBIT - 1057

The different Modes of Introduction provide information about how and when this weakness may be introduced. The Phase identifies a point in the software life cycle at which introduction may occur, while the Note provides a typical scenario related to introduction during the given phase.

Phase	Note
Architecture and Design	
Implementation	

▼ Common Consequences

The table below specifies different individual consequences associated with the weakness. The Scope identifies the application security area that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in exploiting this weakness. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a weakness will be exploited to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Confidentiality	Technical Impact: <i>Read Application Data</i>	

▼ Likelihood Of Exploit

High

▼ Memberships

This MemberOf Relationships table shows additional CWE Categories and Views that reference this weakness as a member. This information is often useful in understanding where a weakness fits within the context of external information sources.

Nature	Type	ID	Name
MemberOf		635	Weaknesses Originally Used by NVD from 2008 to 2016
MemberOf		717	OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling
MemberOf		963	SFP Secondary Cluster: Exposed Data

More information is available — Please select a different filter.

Use of the Common Weakness Enumeration and the associated references from this website are subject to the [Terms of Use](#). For more information, please email cwe@mitre.org.

CWE is sponsored by [US-CERT](#) in the office of [Cybersecurity and Communications](#) at the [U.S. Department of Homeland Security](#). Copyright © 2006-2019, The MITRE Corporation. CWE, CWSS, CWRAP, and the CWE logo are trademarks of [The MITRE Corporation](#).

[Privacy Policy](#)
[Terms of Use](#)
[Site Map](#)
[Contact Us](#)