CWE-668: Exposure of Resource to Wrong Sphere

Weakness ID: 668
Vulnerability Mapping: DISCOURAGED
Abstraction: Class

View customized information: Conceptual | Operational | Mapping Friendly | **Complete** | Custom

▼ Description

The product exposes a resource to the wrong control sphere, providing unintended actors with inappropriate access to the resource.

▼ Extended Description

Resources such as files and directories may be inadvertently exposed through mechanisms such as insecure permissions, or when a program accidentally operates on the wrong object. For example, a program may intend that private files can only be provided to a specific user. This effectively defines a control sphere that is intended to prevent attackers from accessing these private files. If the file permissions are insecure, then parties other than the user will be able to access those files.

A separate control sphere might effectively require that the user can only access the private files, but not any other files on the system. If the program does not ensure that the user is only requesting private files, then the user might be able to access other files on the system.

In either case, the end result is that a resource has been exposed to the wrong party.

▼ Common Consequences

Scope	Impact	Likelihood
Confidentiality Integrity Other	**Technical Impact:** *Read Application Data; Modify Application Data; Other*	

▼ Relationships

▼ *Relevant to the view "Research Concepts" (CWE-1000)*

Nature	Type	ID	Name
ChildOf	P	664	Improper Control of a Resource Through its Lifetime
ParentOf	V	8	J2EE Misconfiguration: Entity Bean Declared Remote
ParentOf	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
ParentOf	B	134	Use of Externally-Controlled Format String
ParentOf	C	200	Exposure of Sensitive Information to an Unauthorized Actor
ParentOf	B	374	Passing Mutable Objects to an Untrusted Method
ParentOf	B	375	Returning a Mutable Object to an Untrusted Caller
ParentOf	C	377	Insecure Temporary File
ParentOf	C	402	Transmission of Private Resources into a New Sphere ('Resource Leak')
ParentOf	B	427	Uncontrolled Search Path Element
ParentOf	B	428	Unquoted Search Path or Element
ParentOf	B	488	Exposure of Data Element to Wrong Session
ParentOf	V	491	Public cloneable() Method Without Final ('Object Hijack')
ParentOf	V	492	Use of Inner Class Containing Sensitive Data
ParentOf	V	493	Critical Public Variable Without Final Modifier
ParentOf	V	498	Cloneable Class Containing Sensitive Information
ParentOf	V	499	Serializable Class Containing Sensitive Data
ParentOf	C	522	Insufficiently Protected Credentials
ParentOf	B	524	Use of Cache Containing Sensitive Information
ParentOf	B	552	Files or Directories Accessible to External Parties
ParentOf	V	582	Array Declared Public, Final, and Static
ParentOf	V	583	finalize() Method Declared Public
ParentOf	V	608	Struts: Non-private Field in ActionForm Class
ParentOf	C	642	External Control of Critical State Data
ParentOf	C	732	Incorrect Permission Assignment for Critical Resource
ParentOf	B	767	Access to Critical Private Variable via Public Method
ParentOf	V	927	Use of Implicit Intent for Sensitive Communication
ParentOf	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
ParentOf	B	1282	Assumed-Immutable Data is Stored in Writable Memory
ParentOf	B	1327	Binding to an Unrestricted IP Address
ParentOf	B	1331	Improper Isolation of Shared Resources in Network On Chip (NoC)
CanFollow	C	441	Unintended Proxy or Intermediary ('Confused Deputy')
CanFollow	V	942	Permissive Cross-domain Policy with Untrusted Domains

▶ *Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)*

▶ *Relevant to the view "Architectural Concepts" (CWE-1008)*

▼ Modes Of Introduction

Phase	Note
Architecture and Design	
Implementation	REALIZATION: This weakness is caused during implementation of an architectural security tactic.
Operation	

▼ Memberships

Nature	Type	ID	Name
MemberOf	C	963	SFP Secondary Cluster: Exposed Data
MemberOf	C	1345	OWASP Top Ten 2021 Category A01:2021 - Broken Access Control
MemberOf	C	1364	ICS Communications: Zone Boundary Failures
MemberOf	C	1403	Comprehensive Categorization: Exposed Resource

▼ Vulnerability Mapping Notes

Usage: DISCOURAGED *(this CWE ID should not be used to map to real-world vulnerabilities)*

Reasons: Frequent Misuse, Abstraction

Rationale:

CWE-668 is high-level and is often misused as a catch-all when lower-level CWE IDs might be applicable. It is sometimes used for low-information vulnerability reports [REF-1287]. It is a level-1 Class (i.e., a child of a Pillar). It is not useful for trend analysis.

Comments:

Closely analyze the specific mistake that is allowing the resource to be exposed, and perform a CWE mapping for that mistake.

▼ Notes

Theoretical

A "control sphere" is a set of resources and behaviors that are accessible to a single actor, or a group of actors. A product's security model will typically define multiple spheres, possibly implicitly. For example, a server might define one sphere for "administrators" who can create new user accounts with subdirectories under /home/server/, and a second sphere might cover the set of users who can create or delete files within their own subdirectories. A third sphere might be "users who are authenticated to the operating system on which the product is installed." Each sphere has different sets of actors and allowable behaviors.

▼ References

[REF-1287] MITRE. "Supplemental Details - 2022 CWE Top 25". Details of Problematic Mappings. 2022-06-28.
<https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25_supplemental.html#problematicMappingDetails>.

▼ Content History

▼ Submissions

Submission Date	Submitter	Organization
2008-04-11 *(CWE Draft 9, 2008-04-11)*	CWE Content Team	MITRE

▶ Modifications

Page Last Updated: July 16, 2024