CWE-284: Improper Access Control

Weakness ID: 284
Vulnerability Mapping: DISCOUNTED

Abstraction: Pillar

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

Description

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Extended Description

Access control involves the use of several protection mechanisms such as:

- Authentication (proving the identity of an actor)
- Authorization (ensuring that a given actor can access a resource), and
- Accountability (tracking of activities that were performed)

When any mechanism is not applied or otherwise fails, attackers can compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc.

There are two distinct behaviors that can introduce access control weaknesses:

- Specification: incorrect privileges, permissions, ownership, etc. are explicitly specified for either the user or the resource (for example, setting a password file to be world-writable, or giving administrator capabilities to a guest user). This action could be performed by the program or the administrator.
- Enforcement: the mechanism contains errors that prevent it from properly enforcing the specified access control requirements (e.g., allowing the user to specify their own privileges, or allowing a syntactically-incorrect ACL to produce insecure settings). This problem occurs within the program itself, in that it does not actually enforce the intended security policy that the administrator specifies.

Alternate Terms

Authorization: The terms "access control" and "authorization" are often used interchangeably, although many people have distinct definitions. The CWE usage of "access control" is intended as a general term for the various mechanisms that restrict which users can access which resources, and "authorization" is more narrowly defined. It is unlikely that there will be community consensus on the use of these terms.

Common Consequences

Scope	Impact	Likelihood
Other	**Technical Impact:** *Varies by Context*	

Potential Mitigations

Phases: Architecture and Design; Operation

Very carefully manage the setting, management, and handling of privileges. Explicitly manage trust zones in the software.

Phase: Architecture and Design

Strategy: Separation of Privilege

Compartmentalize the system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area.

Ensure that appropriate compartmentalization is built into the system design, and the compartmentalization allows for and reinforces privilege separation functionality. Architects and designers should rely on the principle of least privilege to decide the appropriate time to use privileges and the time to drop privileges.

Relationships

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

Nature	Type	ID	Name
MemberOf	V	1000	Research Concepts
ParentOf	C	269	Improper Privilege Management
ParentOf	C	282	Improper Ownership Management
ParentOf	C	285	Improper Authorization
ParentOf	C	286	Incorrect User Management
ParentOf	C	287	Improper Authentication
ParentOf	C	346	Origin Validation Error
ParentOf	B	749	Exposed Dangerous Method or Function
ParentOf	C	923	Improper Restriction of Communication Channel to Intended Endpoints
ParentOf	B	1191	On-Chip Debug and Test Interface With Improper Access Control
ParentOf	B	1220	Insufficient Granularity of Access Control
ParentOf	B	1224	Improper Restriction of Write-Once Bit Fields
ParentOf	B	1231	Improper Prevention of Lock Bit Modification
ParentOf	B	1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
ParentOf	B	1242	Inclusion of Undocumented Features or Chicken Bits
ParentOf	B	1252	CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations
ParentOf	B	1257	Improper Access Control Applied to Mirrored or Aliased Memory Regions
ParentOf	B	1259	Improper Restriction of Security Token Assignment
ParentOf	B	1260	Improper Handling of Overlap Between Protected Memory Ranges
ParentOf	B	1262	Improper Access Control for Register Interface
ParentOf	C	1263	Improper Physical Access Control
ParentOf	B	1267	Policy Uses Obsolete Encoding
ParentOf	B	1268	Policy Privileges are not Assigned Consistently Between Control and Data Agents
ParentOf	B	1270	Generation of Incorrect Security Tokens
ParentOf	B	1274	Improper Access Control for Volatile Memory Containing Boot Code
ParentOf	B	1276	Hardware Child Block Incorrectly Connected to Parent System
ParentOf	B	1280	Access Control Check Implemented After Asset is Accessed
ParentOf	B	1283	Mutable Attestation or Measurement Reporting Data
ParentOf	B	1290	Incorrect Decoding of Security Identifiers
ParentOf	B	1292	Incorrect Conversion of Security Identifiers
ParentOf	C	1294	Insecure Security Identifier Mechanism
ParentOf	B	1296	Incorrect Chaining or Granularity of Debug Components
ParentOf	B	1304	Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation
ParentOf	B	1311	Improper Translation of Security Attributes by Fabric Bridge
ParentOf	B	1312	Missing Protection for Mirrored Regions in On-Chip Fabric Firewall
ParentOf	B	1313	Hardware Allows Activation of Test or Debug Logic at Runtime
ParentOf	B	1315	Improper Setting of Bus Controlling Capability in Fabric End-point
ParentOf	B	1316	Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges
ParentOf	B	1317	Improper Access Control in Fabric Bridge
ParentOf	B	1320	Improper Protection for Outbound Error Messages and Alert Signals
ParentOf	B	1323	Improper Management of Sensitive Trace Data
ParentOf	B	1334	Unauthorized Error Injection Can Degrade Hardware Redundancy

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

Relevant to the view "CISQ Data Protection Measures" (CWE-1340)

Modes Of Introduction

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

Applicable Platforms

Technologies

Class: Not Technology-Specific *(Undetermined Prevalence)*

Class: ICS/OT *(Undetermined Prevalence)*

Observed Examples

Reference	Description
CVE-2022-24985	A form hosting website only checks the session authentication status for a single form, making it possible to bypass authentication when there are multiple forms
CVE-2022-29238	Access-control setting in web-based document collaboration tool is not properly implemented by the code, which prevents listing hidden directories but does not prevent direct requests to files in those directories.
CVE-2022-23607	Python-based HTTP library did not scope cookies to a particular domain such that "supercookies" could be sent to any domain on redirect
CVE-2021-21972	Chain: Cloud computing virtualization platform does not require authentication for upload of a tar format file (CWE-306), then uses .. path traversal sequences (CWE-23) in the file to access unexpected files, as exploited in the wild per CISA KEV.
CVE-2021-37415	IT management product does not perform authentication for some REST API requests, as exploited in the wild per CISA KEV.
CVE-2021-35033	Firmware for a WiFi router uses a hard-coded password for a BusyBox shell, allowing bypass of authentication through the UART port
CVE-2020-10263	Bluetooth speaker does not require authentication for the debug functionality on the UART port, allowing root shell access
CVE-2020-13927	Default setting in workflow management product allows all API requests without authentication, as exploited in the wild per CISA KEV.
CVE-2010-4624	Bulletin board applies restrictions on number of images during post creation, but does not enforce this on editing.

Affected Resources

- File or Directory

Memberships

Nature	Type	ID	Name
MemberOf	C	254	7PK - Security Features
MemberOf	C	723	OWASP Top Ten 2004 Category A2 - Broken Access Control
MemberOf	C	944	SFP Secondary Cluster: Access Management
MemberOf	C	1031	OWASP Top Ten 2017 Category A5 - Broken Access Control
MemberOf	V	1340	CISQ Data Protection Measures
MemberOf	C	1345	OWASP Top Ten 2021 Category A01:2021 - Broken Access Control
MemberOf	C	1369	ICS Supply Chain: IT/OT Convergence/Expansion
MemberOf	C	1372	ICS Supply Chain: OT Counterfeit and Malicious Corruption
MemberOf	C	1396	Comprehensive Categorization: Access Control

Vulnerability Mapping Notes

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

Reasons: Frequent Misuse, Abstraction

Rationale:

CWE-284 is extremely high-level, a Pillar. Its name, "Improper Access Control," is often misused in low-information vulnerability reports [REF-1287] or by active use of the OWASP Top Ten, such as "A01:2021-Broken Access Control". It is not useful for trend analysis.

Comments:

Consider using descendants of CWE-284 that are more specific to the kind of access control involved, such as those involving authorization (Missing Authorization (CWE-862), Incorrect Authorization (CWE-863), Incorrect Permission Assignment for Critical Resource (CWE-732), etc.); authentication (Missing Authentication (CWE-306) or Weak Authentication (CWE-1390)); Incorrect User Management (CWE-286); Improper Restriction of Communication Channel to Intended Endpoints (CWE-923); etc.

Suggestions:

CWE-ID	Comment
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-306	Missing Authentication
CWE-1390	Weak Authentication
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints

Notes

Maintenance

This entry needs more work. Possible sub-categories include:

- Trusted group includes undesired entities (partially covered by CWE-286)
- Group can perform undesired actions
- ACL parse error does not fail closed

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Access Control List (ACL) errors
WASC	2		Insufficient Authorization
7 Pernicious Kingdoms			Missing Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name
CAPEC-19	Embedding Scripts within Scripts
CAPEC-441	Malicious Logic Insertion
CAPEC-478	Modification of Windows Service Configuration
CAPEC-479	Malicious Root Certificate
CAPEC-502	Intent Spoof
CAPEC-503	WebView Exposure
CAPEC-536	Data Injected During Configuration
CAPEC-546	Incomplete Data Deletion in a Multi-Tenant Environment
CAPEC-550	Install New Service
CAPEC-551	Modify Existing Service
CAPEC-552	Install Rootkit
CAPEC-556	Replace File Extension Handlers
CAPEC-558	Replace Trusted Executable
CAPEC-562	Modify Shared File
CAPEC-563	Add Malicious File to Shared Webroot
CAPEC-564	Run Software at Logon
CAPEC-578	Disable Security Software

References

[REF-7] Michael Howard and David LeBlanc. "Writing Secure Code". Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft Press. 2002-12-04. <https://www.microsoftpressstore.com/store/writing-secure-code-9780735617223>.

[REF-44] Michael Howard, David LeBlanc and John Viega. "24 Deadly Sins of Software Security". "Sin 17: Failure to Protect Stored Data." Page 253. McGraw-Hill. 2010.

[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
2006-07-19 *(CWE Draft 3, 2006-07-19)*	PLOVER	

Modifications

Previous Entry Names

Page Last Updated: July 16, 2024