REPORT

Vulnerability Name : Broken access control

CWE : CWE-284: Improper Access Control

|  |
| --- |
|  |

OWSAP Category : A01:2021

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

Business impact: The business impact of the vulnerability "Broken Access Control" can be significant and may pose various risks to an organization. Broken Access Control refers to a situation where users can gain unauthorized access to certain functionalities or data within a system. Here are some potential business impacts associated with this vulnerability

1. Vulnerability Name : cryptographic failures

CWE : **Category ID: 310**

|  |
| --- |
|  |

O WSAP Category : A02:2021

Description : This entry is a Category. Using categories for mapping has been discouraged since 2019. Categories are informal organizational groupings of weaknesses that can help CWE users with data aggregation, navigation, and browsing. However, they are not weaknesses in themselves 1287. This CWE ID may have become widely-used because of NIST's usage in NVD from 2008 to 2016

**Business impact:** Cryptographic issues within a system can have significant business impacts, as cryptography plays a crucial role in securing data, communications, and various aspects of information technology. Here are some potential business impacts associated with cryptographic issues:

Data Breach:

Risk: Weak or compromised encryption can lead to unauthorized access to sensitive data.

Impact: Loss of confidential information, potential legal and regulatory consequences, and damage to the organization's reputation.

Loss of Confidentiality:

Risk: Inadequate encryption may result in the exposure of confidential business data.

Impact: Loss of competitive advantage, potential intellectual property theft, and compromised business secrets.

Integrity Risks:

Risk: Cryptographic weaknesses may allow for data tampering or manipulation.

Impact: Loss of data integrity, compromised trust in business data, and potential financial losses.

Non-Compliance:

Risk: Failure to implement proper cryptographic controls can lead to non-compliance with industry regulations.

Impact: Fines, legal actions, and damage to the organization's reputation due to regulatory violations.

Insecure Communication:

Risk: Weak encryption in communication channels can expose sensitive information to eavesdropping.

Impact: Compromised business communications, loss of sensitive information, and potential damage to business relationships.

Supply Chain Risks:

Risk: Cryptographic vulnerabilities in third-party products or services can pose a risk to the organization's security.

Impact: Disruption of business operations, potential breaches through supply chain partners, and damage to business continuity.

Loss of Trust:

Risk: Customers and stakeholders may lose trust in the organization's ability to secure their information.

Impact: Negative impact on customer relationships, potential loss of business, and damage to brand reputation.

Resource Draining Attacks:

Risk: Cryptographic weaknesses can be exploited for resource-draining attacks, such as denial-of-service attacks.

Impact: Disruption of services, downtime, and potential financial losses.

Legal Consequences:

Risk: Cryptographic issues leading to data breaches may result in legal actions and liabilities.

Impact: Legal expenses, settlements, and potential financial repercussions from legal judgments.

1. Vulnerability Name : Injection

CWE : CWE-94: Improper Control of Generation of Code

OWSAP Category : A03:2021

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

**Business impact**: Code injection vulnerabilities, such as SQL injection and other injection attacks, can have severe business impacts on organizations. These vulnerabilities occur when an attacker is able to inject malicious code into a system, often by manipulating input data. Here are some potential business impacts associated with injection vulnerabilities:

Data Breach:

Risk: Injection attacks can lead to unauthorized access to databases and sensitive information.

Impact: Exposure of confidential data, potential legal consequences, and damage to the organization's reputation.

Data Manipulation:

Risk: Attackers may manipulate or delete data within the database.

Impact: Loss of data integrity, potential financial losses, and disruption of business operations.

Unauthorized Access:

Risk: Injection vulnerabilities can be exploited to gain unauthorized access to systems and applications.

Impact: Unauthorized access to critical systems, potential compromise of privileged information, and risk of further exploitation.

Financial Losses:

Risk: Costs associated with addressing and mitigating the consequences of a security breach.

Impact: Financial losses due to remediation efforts, legal actions, and potential revenue decline.

Reputational Damage:

Risk: News of a security breach can harm the organization's reputation.

Impact: Loss of customer trust, negative publicity, and decreased market value.

Regulatory Compliance Issues:

Risk: Violation of data protection regulations and compliance standards.

Impact: Fines, legal consequences, and damage to the organization's compliance record.

Business Disruption:

Risk: Injection attacks can lead to the disruption of business-critical applications.

Impact: Downtime, loss of productivity, and potential financial losses.

Intellectual Property Theft:

Risk: Injection vulnerabilities may be exploited to steal intellectual property or proprietary information.

Impact: Loss of competitive advantage, damage to innovation, and potential legal consequences.

Identity Theft:

Risk: Injection attacks targeting user authentication systems may lead to identity theft.

Impact: Compromised user accounts, financial losses, and damage to customer relationships.

Supply Chain Risks:

Risk: Injection vulnerabilities in third-party components can pose a risk to the organization's security.

Impact: Disruption of business operations, potential breaches through supply chain partners, and damage to business continuity.

To mitigate the business impact of injection vulnerabilities, organizations should implement secure coding practices, input validation, and parameterized queries to prevent injection attacks. Regular security audits, penetration testing, and continuous monitoring are essential for identifying and addressing injection vulnerabilities in a timely manner. Additionally, employee training and awareness programs can help prevent security lapses that may lead to injection attacks.

4.Vulnerability Name : Insecure design

CWE : CWE- A04:2021 – Insecure Design

|  |
| --- |
|  |

OWSAP Category : A04:2021

Description : Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

**Business impact:** Collect and negotiate the business requirements for an application with the business, including the protection requirements concerning confidentiality, integrity, availability, and authenticity of all data assets and the expected business logic. Take into account how exposed your application will be and if you need segregation of tenants (additionally to access control). Compile the technical requirements, including functional and non-functional security requirements. Plan and negotiate the budget covering all design, build, testing, and operation, including security activities.

5. Vulnerability Name : misconfiguration

CWE : CWE CATEGORY: Configuration

OWSAP category: : A05:2021

Description : his entry is a Category. Using categories for mapping has been discouraged since 2019. Categories are informal organizational groupings of weaknesses that can help CWE users with data aggregation, navigation, and browsing. However, they are not weaknesses in themselves . This CWE entry may have become widely-used because of NIST's usage in NVD from 2008 to 2016 (see  view, updated to the  view in 2016). Mapping is also Prohibited because this entry's status is Obsolete

6 Vulnerability Name : vulnerable and outdated components

CWE : CWE-1395: Dependency on Vulnerable Third-Party Component

|  |
| --- |
|  |

OWSAP Category : A06:2021

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

Business impact: Many products are large enough or complex enough that part of their functionality uses libraries, modules, or other intellectual property developed by third parties who are not the product creator. For example, even an entire operating system might be from a third-party supplier in some hardware products. Whether open or closed source, these components may contain publicly known vulnerabilities that could be exploited by adversaries to compromise the product.

7. Vulnerability Name : :  Identification and Authentication Failures

## CWE : CWE-1353:  Identification and Authentication Failures

OWSAP Category : A07:2021

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

Business impact: : Many products are large enough or complex enough that part of their functionality uses libraries, modules, or other intellectual property developed by third parties who are not the product creator. For example, even an entire operating system might be from a third-party supplier in some hardware products. Whether open or closed source, these components may contain publicly known vulnerabilities that could be exploited by adversaries to compromise the product.

8.

Vulnerability Name : software and data integrity failures

CWE : 1344 weakness om owasp

OWSAP Category : A08:2021

Description :

This entry is a Category. Using categories for mapping has been discouraged since 2019. Categories are informal organizational groupings of weaknesses that can help CWE users with data aggregation, navigation, and browsing. However, they are not weaknesses in themselves.

Business impact: This entry is a Category. Using categories for mapping has been discouraged since 2019. Categories are informal organizational groupings of weaknesses that can help CWE users with data aggregation, navigation, and browsing. However, they are not weaknesses in themselves.

9.Vulnerability Name : security monitoring and logging failures

CWE : CWE-778: Insufficient Logging

OWSAP Category : A09:2021

Description : When a security-critical event occurs, the product either does not record the event or omits important details about the event when logging it.

Business impact: When security-critical events are not logged properly, such as a failed login attempt, this can make malicious behavior more difficult to detect and may hinder forensic analysis after an attack succeeds.

As organizations adopt cloud storage resources, these technologies often require configuration changes to enable detailed logging information, since detailed logging can incur additional costs. This could lead to telemetry gaps in critical audit logs. For example, in Azure, the default value for logging is disabled.

|  |  |
| --- | --- |
|  |  |
|  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |