Vulnerability Name: Unquoted Search Path or Element

CWE: CWE-428

OWASP Category: A1: Injection

Description: The product uses a search path that contains an unquoted element, in which the element contains whitespace or other separators. This can cause the product to access resources in a parent path.

Business impact: CWE-428, the "Unquoted Search Path or Element" vulnerability, can result in serious business impacts:

**Security Risks:** It opens the door to security breaches and unauthorized access.

**Operational Disruption:** Exploitation can lead to downtime and loss of productivity.

**Legal and Compliance Issues:** Non-compliance may result in legal penalties and regulatory fines.

**Reputation Damage**: Trust and reputation can be severely damaged.

**Financial Costs**: Remediation and recovery can be costly.

**Competitive Disadvantage:** Weaker security may put the business at a disadvantage compared to more secure competitors.

Vulnerability Name: Out-of-bounds Write

CWE: CWE-787

OWASP Category: A7: Security Misconfiguration

Description: The product writes data past the end, or before the beginning, of the intended buffer. Typically, this can result in corruption of data, a crash, or code execution. The product may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent write operation then produces undefined or unexpected results.

Business impact: CWE-787, "Out-of-bounds Write," can have significant business impacts, including:

1. Security Breaches: Exploiting this vulnerability can lead to unauthorized data manipulation, system crashes, or even remote code execution, potentially compromising sensitive information.

2. Loss of Customer Trust: Security incidents resulting from CWE-787 can erode trust and damage a company's reputation, leading to customer loss.

3. Operational Disruption: Addressing and recovering from security breaches can cause downtime and productivity loss, impacting business operations.

4. Legal and Compliance Issues: Non-compliance with data protection regulations may result in legal penalties and regulatory fines.

5. Financial Costs: Remediation and recovery can be costly, including expenses for forensics, legal, and reputation management.

6. Competitive Disadvantage: Businesses with a history of security vulnerabilities may lose customers to more secure competitors.

Vulnerability Name: Improper Authentication

CWE:

CWE-287

OWASP Category: A2: Broken Authentication

Description: When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

Business impact:

CWE-287, "Improper Authentication," can have several significant business impacts when not properly addressed:

Unauthorized Access: Improper authentication can lead to unauthorized individuals gaining access to sensitive systems or data, potentially resulting in data breaches, theft, or unauthorized actions.

Data Breaches: If attackers exploit authentication weaknesses, they can gain access to sensitive customer or business data, leading to costly data breaches, legal consequences, and damage to a company's reputation.

Loss of Trust: Security incidents involving improper authentication erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

Legal and Regulatory Consequences: Non-compliance with data protection and privacy regulations can result in fines, legal actions, and other regulatory penalties, further impacting the company's financial health.

Operational Disruption: Remediation efforts, including resetting user accounts or implementing stronger authentication mechanisms, can cause operational disruptions and productivity loss.

Vulnerability Name: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CWE: CWE-78

OWASP Category: A1: Injection

Description: The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.

Business impact: CWE-78, which relates to "OS Command Injection," can have several significant business impacts when not properly mitigated:

Unauthorized Access: Command injection vulnerabilities can allow attackers to execute arbitrary commands on a system, potentially leading to unauthorized access and data breaches.

Data Loss or Manipulation: Attackers exploiting this vulnerability may manipulate data, delete critical information, or even compromise the integrity of the system, resulting in data loss and operational disruptions.

Loss of Trust: Security incidents involving OS command injection erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

Legal and Regulatory Consequences: Non-compliance with data protection and privacy regulations can result in fines, legal actions, and other regulatory penalties, further impacting the company's financial health.

Operational Disruption: Remediation efforts and recovery from a successful attack can cause operational disruptions, resulting in productivity loss.

Vulnerability Name: Observable Discrepancy

CWE: CWE-203

OWASP Category: Observable Differences Based on Input

Description: The product behaves differently or sends different responses under different circumstances in a way that is observable to an unauthorized actor, which exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not.

Discrepancies can take many forms, and variations may be detectable in timing, control flow, communications such as replies or requests, or general behavior. These discrepancies can reveal information about the product's operation or internal state to an unauthorized actor. In some cases, discrepancies can be used by attackers to form a side channel.

Business impact: CWE-203, "Observable Differences Based on Input," is a type of information leakage vulnerability. While this particular CWE may not be as well-known as some other common vulnerabilities, it can still have business impacts:

Data Exposure: Observable differences based on input can inadvertently reveal sensitive information, such as internal data structures, error messages, or system behavior. This exposure can provide valuable information to attackers.

Security Risk: The information leakage can be used by malicious actors to plan and execute targeted attacks. It may help attackers understand the inner workings of a system, identify weaknesses, and devise a more effective attack strategy.

Loss of Competitive Advantage: If proprietary information or unique data structures are exposed, it can undermine a company's competitive advantage, potentially leading to imitations by competitors.

Regulatory Non-Compliance: Depending on the type of data exposed, CWE-203 may result in non-compliance with data protection regulations and privacy laws. Non-compliance can lead to legal penalties and damage an organization's reputation.

Reputation Damage: Information disclosure vulnerabilities can undermine trust in an organization's ability to protect sensitive data, potentially damaging its reputation with customers and partners.

Vulnerability Name: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE: CWE-22

OWASP Category: A4: XML External Entities (XXE)

Description: The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

Business impact: CWE-22, "Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)," can have several significant business impacts when not properly mitigated:

Data Exposure: Path traversal vulnerabilities can allow attackers to access and retrieve sensitive files or data from the server. This exposure can lead to data breaches and unauthorized access to confidential information.

Loss of Confidentiality: If sensitive data, such as customer records, intellectual property, or financial information, is exposed, it can result in a loss of confidentiality and legal consequences.

Regulatory Non-Compliance: Depending on the type of data exposed, CWE-22 may lead to non-compliance with data protection regulations and privacy laws, resulting in legal penalties and damage to the company's reputation.

Operational Disruption: Remediation efforts, including securing the application and investigating the breach, can disrupt business operations and lead to productivity loss.

Reputation Damage: Data breaches and improper handling of sensitive information can damage an organization's reputation, causing customers and partners to lose trust in the company's ability to protect their data.

Financial Costs: Remediation, legal, and public relations costs associated with path traversal vulnerabilities can be substantial, affecting the company's bottom line.

Vulnerability Name: Inappropriate Encoding for Output Context

CWE: CWE-838

OWASP Category: Security Misconfiguration

Description: The product uses or specifies an encoding when generating output to a downstream component, but the specified encoding is not the same as the encoding that is expected by the downstream component.

Business impact: CWE-838, "Inappropriate Access of Resource Through Identifying Information," typically occurs when an application improperly handles sensitive data, leading to business risks and impacts:

Data Exposure: Inappropriate access can result in unauthorized parties gaining access to sensitive data, including customer records, financial information, or intellectual property.

Loss of Confidentiality: The exposure of sensitive data may lead to a loss of confidentiality, resulting in legal consequences and damage to the company's reputation.

Regulatory Non-Compliance: If the unauthorized access violates data protection or privacy regulations, it can result in legal penalties, regulatory fines, and additional damage to the organization's reputation.

Operational Disruption: Efforts to secure the application and investigate the breach can disrupt business operations, causing productivity loss.

Reputation Damage: Data breaches and improper handling of sensitive information can damage the organization's reputation, eroding trust in its ability to protect data.

Vulnerability Name: Incorrect Authorization

CWE: CWE-863

OWASP Category: Access Control

Description: The product uses or specifies an encoding when generating output to a downstream component, but the specified encoding is not the same as the encoding that is expected by the downstream component.

Business impact:

CWE-863, "Incorrect Authorization," can lead to unauthorized access, data breaches, legal consequences, operational disruptions, reputation damage, financial costs, and a competitive disadvantage. Improper authorization can result in data exposure, privacy violations, regulatory non-compliance, and eroded trust, impacting the company's integrity and success.

Vulnerability Name: Exposure of Sensitive Information to an Unauthorized Actor

CWE: CWE-200

OWASP Category: Sensitive Data Exposure

Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business impact:

CWE-200, "Exposure of Sensitive Information to an Unauthorized Actor," can have severe business impacts when not properly mitigated:

Data Breaches: The exposure of sensitive information can lead to data breaches, resulting in unauthorized access to confidential data, including customer records and financial information.

Loss of Trust: Security incidents involving sensitive data exposure erode trust in a business or service. Customers, partners, and stakeholders may lose confidence in the organization's ability to protect their information.

Legal and Regulatory Consequences: Non-compliance with data protection regulations can result in fines, legal actions, and other regulatory penalties, further impacting the company's financial health.

Reputation Damage: Data breaches and the mishandling of sensitive information can damage the organization's reputation, causing customers and partners to lose trust.

Vulnerability Name: Incorrect Permission Assignment for Critical Resource

CWE: CWE-732

OWASP Category: Security Misconfiguration

Description: The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

When a resource is given a permission setting that provides access to a wider range of actors than required, it could lead to the exposure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution, or sensitive user data. For example, consider a misconfigured storage account for the cloud that can be read or written by a public or anonymous user.

Business impact:

CWE-732, "Insecure Permission Assignment for Critical Resource," can have significant business impacts, including unauthorized access to critical resources, data breaches, operational disruption, legal consequences, financial costs, reputation damage, and competitive disadvantages. Failing to secure access to critical resources can lead to data exposure, regulatory fines, trust erosion, and loss of business opportunities, negatively affecting the organization's integrity and success.