Stage 1

1. CWE-284: Improper Access Control

OWASP CATEGORY: A01 2021 Broken Access Control

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

Business Impact: Improper Access Control vulnerabilities can have significant business impact, potentially leading to unauthorized access to sensitive data, financial losses due to fraudulent activities, regulatory penalties, damaged reputation eroding customer trust, intellectual property theft, operational disruptions, legal repercussions, and increased operational costs for incident mitigation, underscoring the critical need for robust access control measures to mitigate these risks and protect overall business integrity.

2. CWE-326: Inadequate Encryption Strength

OWASP CATEGORY: A02 2021 Cryptographic Failures

Description: The product stores or transmits sensitive data using an encryption scheme that is theoretically sound but is not strong enough for the level of protection required.

Business Impact: This vulnerability can lead to critical business ramifications. Insufficient encryption strength exposes sensitive data to potential breaches, allowing unauthorized parties to compromise confidentiality and integrity. As a result, customer trust can erode, leading to diminished loyalty and potential revenue loss. Regulatory compliance may be compromised, resulting in fines and legal consequences. The organization's reputation can suffer severe damage, affecting brand value and market standing. Intellectual property theft becomes a heightened risk, threatening innovation, and competitiveness. Remediation efforts, legal actions, and customer breach notifications incur substantial costs. In essence, this vulnerability jeopardizes both financial stability and the trust of stakeholders, highlighting the urgent need for robust encryption measures that align with data sensitivity.

3. CWE-94: Improper Control of Generation of Code ('Code Injection')

OWASP CATEGORY: A03 2021 Injection

Description: The product constructs all or part of a code segment using externally influenced input from an upstream component, butit does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Business Impact: This vulnerability holds the potential to profoundly affect the business landscape. The manipulation of code syntax or behavior through externally influenced input can lead to security breaches, system vulnerabilities, and unauthorized access to critical functionalities. Malicious actors exploiting this weakness can compromise sensitive data, disrupt operations, and even gain control over systems, resulting in financial losses, tarnished reputation, and potential legal liabilities. Customer trust can be eroded due to breaches and data exposure, potentially leading to customer churn and decreased revenue. Regulatory non-compliance and associated penalties are possible outcomes, impacting the organization's financial health. The costs of incident response, remediation, legal actions, and potential regulatory fines can escalate rapidly. In essence, this vulnerability jeopardizes business continuity, reputation, and financial stability, underscoring the necessity for robust input validation and code construction practices to prevent unauthorized manipulation and subsequent adverse business outcomes.

4. CWE-657: Violation of Secure Design Principles

OWASP CATEGORY: A04 2021 Insecure design

Description: The product violates well-established principles for secure design.

Business Impact: This vulnerability can have wide-ranging implications for the business. Violations of well-established secure design principles can create weak points in the product's architecture, making it susceptible to various forms of exploitation. These vulnerabilities can lead to unauthorized access, data breaches, and compromised user privacy. Financial losses can stem from the costs of incident response, remediation, legal actions, and potential regulatory fines. The organization's reputation can suffer due to perceived negligence in safeguarding customer information and adhering to industry best practices. Customer trust may erode, resulting in reduced customer loyalty and potential revenue decline. The product's competitiveness in the market can also be hampered if security weaknesses become widely known. Regulatory compliance breaches can result in legal liabilities and financial penalties. Ultimately, this vulnerability has the potential to disrupt business operations, damage brand reputation, and lead to enduring financial repercussions. It underscores the critical importance of following established secure design principles to mitigate risks and safeguard both the organization's assets and its reputation.

5. CWE-942: Permissive Cross-domain Policy with Untrusted Domains

OWASP CATEGORY: A05 2021 Security Misconfiguration

Description: The product uses a cross-domain policy file that includes domains that should not be trusted.

Business Impact: This vulnerability introduces substantial potential consequences for the business. Inclusion of untrustworthy domains within a cross-domain policy file can lead to unauthorized data access, data leakage, and potentially facilitate cross-site scripting (XSS) attacks. These security weaknesses can result in compromised customer data, eroding trust and potentially leading to customer attrition. Malicious actors exploiting this vulnerability might gain unauthorized access to sensitive functionalities, leading to system disruptions and financial losses. Regulatory compliance may be compromised, resulting in penalties and legal liabilities. The costs associated with incident response, mitigation, and potential legal actions can escalate rapidly. The organization's reputation can be damaged due to perceived negligence in protecting customer information and adhering to security best practices. Market competitiveness can also suffer if the vulnerability becomes public knowledge. In essence, this vulnerability threatens both customer trust and the organization's bottom line, underscoring the critical need for thorough validation and controlled domain inclusion within cross-domain policy files to prevent unauthorized access and potential breaches.

6. CWE-1104: Use of Unmaintained Third-Party Components

OWASP CATEGORY: A06 2021 vulnerable and outdated components

DESCRIPTION: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

BUSINESS IMPACT: Utilizing unmaintained third-party components within your business can expose you to a range of detrimental outcomes. These include heightened security vulnerabilities, increased maintenance complexities, potential compatibility issues, performance deficiencies, legal risks stemming from outdated licensing, and a lack of access to valuable new features. While there might be initial cost savings, the long-term drawbacks such as compromised security, stability, and growth potential far outweigh any immediate benefits. To mitigate these risks, regular audits, vigilant security monitoring, vendor communication, and a preference for actively supported alternatives are essential strategies.

7. CWE-287: Improper Authentication

OWASP CATEGORY: A07 2021 Identification and Authentication Failures

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: The relevant Common Weakness Enumeration (CWE) entry for identification and authentication failure is CWE-287: Improper Authentication. This weakness encompasses issues where an application or system fails to properly authenticate users, leading 3to unauthorized access and potential security breaches. It includes scenarios where authentication mechanisms are implemented incorrectly, credentials are stored or transmitted insecurely, or authentication bypass vulnerabilities exist. Proper authentication is crucial for ensuring the security of systems and protecting sensitive data from unauthorized access.

8. CWE-502: Deserialization of Untrusted Data

OWASP CATEGORY: A08 2021 Software and Data Integrity Failures

Description: The product deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

BUSINESS IMPACT: For software and data integrity failures, the relevant Common Weakness Enumeration (CWE) entry is CWE-367: Time-of-Check Time-of-Use (TOCTOU) Race Condition. This weakness involves situations where a system's security or integrity is compromised due to the time gap between checking a resource's state and using it, allowing attackers to manipulate the resource in that window. This can lead to unauthorized data modification, bypassing security measures, and other integrity-related issues. Addressing time-of-check time-of-use race conditions is essential for maintaining the integrity and security of software and data.

9. CWE-778: Insufficient Logging

OWASP CATEGORY: A09 2021 Security Logging and Monitoring Failures

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: Security logging and monitoring failures can result in severe business consequences, including delayed detection of cyber threats, inability to respond effectively to breaches, compromised compliance with regulations, loss of sensitive data without detection, damage to reputation and customer trust, increased legal and financial liabilities due to inadequate evidence in

case of incidents, decreased operational efficiency due to manual incident investigation, and heightened vulnerability to persistent attacks due to lack of real-time threat visibility. This underscores the critical importance of robust security logging and monitoring practices to safeguard against these damaging effects and ensure proactive threat detection and response.

10. CWE-352: Cross-Site Request Forgery (CSRF)

OWASP CATEGORY: A10 2021 - Server-Side Request Forgery

Description: The web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.

Business Impact: Server-Side Request Forgery (SSRF) can have serious business implications, including exposure of sensitive data, unauthorized access to internal resources, network scanning, service disruptions, reputation damage, regulatory non-compliance, financial loss, and operational costs. Successful SSRF attacks can lead to data manipulation, privilege escalation, lawsuits, and erosion of user trust, necessitating robust security measures, regular audits, and employee training to prevent and mitigate these risks effectively.