***6.1 Vulnerability Report:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability Name | CWE No. | OWASP/SANS Category | Description | Business Impact |
| SSL Certificate cannot be trusted | 295 | OWASP A6: Security Misconfiguration | This vulnerability arises when the SSL certificate presented by the server is not trusted by the client. | |  |  | | --- | --- | |  | Can lead to Man-in-the-Middle (MitM) attacks, resulting in data breaches and loss of sensitive information. | |
| Node.js version related multiple issues | 1104 | |  | | --- | | OWASP A9: Using Components with Known Vulnerabilities | | Multiple vulnerabilities exist due to the use of outdated Node.js versions | Can lead to various security issues, including code execution and denial of service, impacting application availability. |
| Open JDK 8<=8U432/  17.0.0<=17.0 <=21.0.5/  23.0.1 vulnerability | 21502 | OWASP A9: Using Components with Known Vulnerabilities | Vulnerabilities in outdated versions of open JDK can lead to security  Issues such as information disclosure, unauthorised access and other security flaws. | May lead to compromised application security , data breaches, and potential legal and regulatory implications. |
| Apache HTTP server site enumeration | 200 | OWASP A6: Security Misconfigurations. | This vulnerability allows attackers to enumerate sites hosted on an Apache HTTP server, revealing potentially sensitive information about the server configuration and hosted sites. | Can result in information leakage and provide attackers with insights to plan further attacks on the server and its applications. |
| Node.js 18.x < 18.20.1/20.x < 20.12.1/<21.7.2 multiple vulnerabilities | 400  352  20 | OWASP A9: Using Components with Known Vulnerabilities | Multiple vulnerabilities in these Node.js versions include issues like uncontrolled resource consumption, cross-site request forgery (CSRF), and improper input validation. | May lead to denial of service, unauthorized actions, and potentially compromise the application’s integrity and availability. |