```
# Nessus Web Application Vulnerability Report Solutions

**Report Date: November 13, 2024**

**Host: 13.52.135.157**

**Application: shopcart**

**Vulnerability 1: Jenkins LTS < 2.303.3 / Jenkins weekly < 2.319 Multiple Vulnerabilities (Plugin ID 154894)**

**Description: Multiple vulnerabilities affecting agent-to-controller communication and file path filtering.**

**Solution: Upgrade Jenkins to Weekly version 2.319 or later, or LTS version 2.303.3 or later. This addresses all reported CVEs (2021-21685 to 2021-21698).**

**Vulnerability 2: Jenkins LTS < 2.332.4 / Jenkins weekly < 2.356 Multiple Vulnerabilities (Plugin ID 163258)**

**Description: Multiple Cross-Site Scripting (XSS) vulnerabilities, authentication bypass, and information disclosure issues.**

**Solution: Upgrade Jenkins to Weekly version 2.356 or later, or LTS version 2.332.4 or 2.346.1 or later. This mitigates the identified XSS, authentication bypass, and unsafe file handling vulnerabilities (CVE-2022-34170 to CVE-2022-34213). Review and address listed plugins that lack fixes. Consider implementing Content Security Policy (CSP) to further mitigate XSS risks.**

**Vulnerability 3: Jenkins LTS < 2.426.3 / Jenkins weekly < 2.442 Multiple Vulnerabilities (Plugin IDs 172394 & 189463)**

**Description: Arbitrary file read via CLI, and Cross-Site WebSocket Hijacking (CSWSH).**

**Solution: Upgrade Jenkins to Weekly version 2.442 or later, or LTS version 2.426.3 or later. This addresses the CLI file read (CVE-2024-23897) and**
```

CSWSH (CVE-2024-23898) vulnerabilities.

Vulnerability 4: Jenkins < (2.204.6 / 2.222.1) LTS / 2.228 Multiple Vulnerabilities (Plugin ID 135178)

Description: Authentication bypass and stored XSS vulnerabilities.

Solution: Upgrade Jenkins to version 2.228 or later, or LTS version 2.204.6 or 2.222.1 or later.

Vulnerability 5: Jenkins < 2.164.2 LTS / 2.172 Multiple Vulnerabilities (Plugin ID 124168)

Description: Authentication bypass and cross-site scripting vulnerabilities.

Solution: Upgrade Jenkins to version 2.172 or later, or LTS version 2.164.2 or later.

Vulnerability 6: Jenkins < 2.176.2 LTS / 2.186 Multiple Vulnerabilities (Plugin ID 127053)

Description: Arbitrary file write, security bypass, and information disclosure vulnerabilities.

Solution: Upgrade Jenkins to version 2.186 or later, or LTS version 2.176.2 or later. Restrict file upload destinations to within the designated workspace.

Vulnerability 7: Jenkins < 2.176.3 LTS / 2.192 Multiple Vulnerabilities (Plugin ID 129776)

Description: Stored XSS in update center and Cross-Site Request Forgery (CSRF) vulnerability.

Solution: Upgrade Jenkins to version 2.192 or later, or LTS version 2.176.3 or later. Ensure update center URLs are trusted sources. Implement CSRF protection mechanisms such as Anti-CSRF tokens.

Vulnerability 8: Jenkins < 2.263.2 LTS / 2.275 Multiple Vulnerabilities (Plugin

ID 145248)

Description: Agent name manipulation, potential unsafe object instantiation, and URL access bypass.

Solution: Upgrade Jenkins to version 2.275 or later, or LTS version 2.263.2 or later. Carefully validate agent names and review Old Data Monitor configurations for potentially unsafe objects.

Vulnerability 9: Jenkins LTS < 2.277.3 / Jenkins weekly < 2.286 (Plugin ID 148975)

Description: Eclipse Jetty CPU exhaustion vulnerability.

Solution: Upgrade Jenkins to Weekly version 2.286 or later, or LTS version 2.277.3 or later.

Vulnerability 10: Jenkins LTS < 2.289.2 / Jenkins weekly < 2.300 Multiple Vulnerabilities (Plugin ID 151193)

Description: Unauthorized job cancellation, session fixation, XML external entity (XXE) injection, phishing risk, and unauthorized information disclosure.

Solution: Upgrade Jenkins to Weekly version 2.300 or later, or LTS version 2.289.2 or later. Review Item/Cancel permissions. Enforce session invalidation on login. Configure XML parsers to prevent XXE. Validate redirect URLs and restrict them to Jenkins URLs. Ensure proper authorization checks for sensitive HTTP endpoints.

Vulnerability 11: Jenkins LTS < 2.319.2 / Jenkins weekly < 2.330 Multiple Vulnerabilities (Plugin ID 156929)

Description: CSRF vulnerabilities and various other issues in multiple plugins.

Solution: Upgrade Jenkins to Weekly version 2.330 or later, or LTS version 2.319.2 or later. Implement appropriate CSRF protection mechanisms and address specific vulnerabilities in affected plugins as outlined in the Nessus

report.

Vulnerability12: JenkinsLTS < 2.319.3 / Jenkinsweekly < 2.334 Multiple Vulnerabilities(PluginID 157860)

Description:XStreamvulnerabilitiesleadingto potentialdenial-of-serviceand resourceexhaustion.

Solution:UpgradeJenkinsto Weekly version2.334 or later,or LTS version 2.319.3 or later.ConsidersettingXStreamto NO_REFERENCEmode as a workaroundf upgradingis not immediatelypossible.

Vulnerability13: JenkinsLTS < 2.361.1 / Jenkinsweekly < 2.363 (PluginID 164898)

Description:Eclipse Jettyresourceexhaustionvulnerabilitydue to impropererror handling.

Solution:UpgradeJenkinsto Weekly version2.363 or later,or LTS version 2.361.1 or later.

Vulnerability14: JenkinsLTS < 2.401.1 / Jenkinsweekly < 2.400 XSRF (Plugin ID 177395)

Description:Cross-siterequestforgery(CSRF)vulnerabilityin contextmenu handling.

Solution:UpgradeJenkinsto Weekly version2.400 or later,or LTS version 2.401.1 or later.ImplementCSRF protectionmechanisms.

Vulnerability15: JenkinsLTS < 2.414.2 / Jenkinsweekly < 2.424 Multiple Vulnerabilities(PluginID 181682)

Description:Sensitive buildvariableexposureandinsecuretemporaryfile handling.

Solution:UpgradeJenkinsto Weekly version2.424 or later,or LTS version

2.414.2 or later. Review build history widget configurations to avoid exposure of sensitive variables. Configure Jenkins to use a secure temporary directory with appropriate permissions.

Vulnerability16: JenkinsLTS < 2.414.3 / Jenkinsweekly < 2.428 Multiple Vulnerabilities(PluginID 183316)

Description:Eclipse Jettyvulnerabilitiesrelatedto HTTP/2headerhandlingand denial-of-service(DoS).

Solution:UpgradeJenkinsto Weekly version2.428 or later,or LTS version 2.414.3 or laterto addressthe Eclipse JettyDoS. Implementratelimitingand resourceconstraintsto mitigateHTTP/2DoS attacks.

Vulnerability17: JenkinsLTS < 2.440.2 / Jenkinsweekly < 2.444 (PluginID 192307)

Description:Jettyfile descriptorexhaustionvulnerability.

Solution:UpgradeJenkinsto Weekly version2.444 or later,or LTS version 2.440.2 or later.

Vulnerability18: JenkinsLTS < 2.452.4 / Jenkinsweekly < 2.471 Multiple Vulnerabilities(PluginID 205143)

Description:Arbitraryfile readvia ClassLoaderProxyandunauthorizedaccess to My Views.

Solution:UpgradeJenkinsto Weekly version2.471 or later,or LTS version 2.452.4 or2.462.1 or later.

Vulnerability19: JenkinsLTS < 2.462.3 / Jenkinsweekly < 2.479 Multiple Vulnerabilities(PluginID 208098)

Description: Secretdisclosurein errormessages anditem creationbypass.

Solution:UpgradeJenkinsto Weekly version2.479 or later,or JenkinsLTS

version 2.462.3 or later.

Vulnerability 20: HSTS Missing from HTTPS Server (Plugin ID 142960 and 84502)

Description: HTTP Strict Transport Security (HSTS) not enforced.

Solution: Configure the web server (likely Apache in this case, given plugin 48204) to send the `Strict-Transport-Security` header. Example: `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`.

Vulnerability 21: HTTP Cookie 'secure' Property Transport Mismatch (Plugin ID 69826 and 85602)

Description: Cookies lacking the 'secure' flag, potentially exposing them over HTTP.

Solution: Add the 'secure' attribute to all cookies, especially JSESSIONID, to ensure they are only sent over HTTPS. In application code, set the secure flag when creating the cookie. Example (Java): `Cookie cookie = new Cookie("JSESSIONID", sessionId); cookie.setSecure(true); response.addCookie(cookie);`.

Vulnerability 22: Apache HTTP Server Version Disclosure (Plugin ID 48204)

Description: Apache HTTP server version is disclosed in banners.

Solution: Configure Apache to suppress version information in server banners and error messages. In your Apache configuration file (e.g., httpd.conf or apache2.conf), modify the `ServerTokens` and `ServerSignature` directives. For example:
`ServerTokens Prod` and `ServerSignature Off`.

Vulnerability 23: Web Server robots.txt Information Disclosure (Plugin ID

10302)

Description: robots.txt file discloses potentially sensitive directories.

Solution: Review the contents of robots.txt. Remove any entries that unintentionally reveal sensitive directories. If robots.txt is not intentionally being used, remove the file or configure the web server to not serve it. Alternatively, use robots meta tags within HTML pages to control indexing.

General Recommendations:

* **Regular Updates: Keep Jenkins and all its plugins updated to the latest versions to patch known vulnerabilities.**
* **Security Hardening: Review and apply Jenkins security best practices, such as implementing role-based access control, configuring security realms, and enabling CSRF protection globally.**
* **Penetration Testing: Conduct regular penetration testing to identify and address any vulnerabilities that might not be detected by automated scanners.**
* **Web Application Firewall (WAF): Consider deploying a WAF to provide additional protection against web application attacks.**
* **Monitoring and Logging: Implement comprehensive monitoring and logging to detect suspicious activity and security incidents.**

This document provides solutions for the identified vulnerabilities. It should be implemented and retested to ensure effectiveness. Each solution should be applied with consideration for the specific environment and application context.

```
```