2.7 129776 - Jenkins < 2.176.3 LTS / 2.192 Multiple Vulnerabilities (FIXED by Jenkins upgrade)

* **Description:** Stored XSS in the update center and cross-site request forgery (XSRF).
* **Solution:** Addressed by upgrading Jenkins.

**2.8 145248, 148975, 151193, 156929, 157860, 164898, 177395, 178903, 181682, 183316, 192307, 1

These vulnerabilities cover a wide range of issues, including CSRF, XSS, information disclosure, authe

* **Solution:** Upgrading Jenkins addresses most of these. Refer to the specific plugin recommendatio

3. HTTP Security Hardening

3.1 142960, 84502 - HSTS Missing From HTTPS Server (RFC 6797)

* **Description:** The web server is not enforcing HTTP Strict Transport Security (HSTS).
* **Solution:** Configure your web server to enforce HSTS. This involves adding the `Strict-Transport-S
    `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`

**3.2 69826 - HTTP Cookie 'secure' Property Transport Mismatch, 85602 - Web Application Cookies N

* **Description:** Cookies are not consistently marked with the `Secure` flag, which can lead to their tra
* **Solution:** Ensure that all cookies, especially session cookies, are marked with the `Secure` flag. T

3.3 43111 - HTTP Methods Allowed (per directory)

* **Description:** Informational plugin output regarding allowed HTTP methods. Not necessarily a vuln
* **Solution:** Review the output. If unnecessary or insecure HTTP methods are enabled (PUT, DELE

**3.4 10107 - HTTP Server Type and Version, 48204 - Apache HTTP Server Version, 194915 - Eclipse

* **Description:** Informational plugins revealing web server details. Consider minimizing information l