**Vulnerability Report**

**Name:** Prasad Jadhav

**Vulnerability Title:** WordPress JetPack Plugin Arbitrary File Manipulation Vulnerability  
**Plugin ID:** 1.3.6.1.4.1.25623.1.0.127450  
**CVE ID:** CVE-2023-2996  
**Host Scanned:** 192.168.1.72 (mr robot)  
**Tool Used:** OpenVAS  
**Scan Date:** May 6, 2025

1. **Description:** The WordPress **JetPack** plugin prior to version 3.3.6 suffers from an **arbitrary file manipulation vulnerability**. Due to insufficient validation of uploaded files, an attacker with at least an author role can overwrite or delete arbitrary files on the server. In some edge cases, it can lead to Remote Code Execution (RCE) through exploitation of PHP **phar deserialization** when combined with additional gadgets present in the environment.
2. **Risk Summary:**

* Risk Factor: Critical
* CVSS v3.0 Base Score: 8.8 (High)
* Attack Vector: Network
* Impact:
  + Arbitrary file deletion
  + Overwriting application files
  + Potential Remote Code Execution
* Exploitable Remotely: Yes
* Authentication Required: Yes (Author role or higher)

1. **Affected Software/Services:**

* Plugin Name: JetPack
* Affected Version: ≤ 3.3.2
* Fixed Version: 3.3.6
* Installation Path: /wp-content/plugins/jetpack
* Platform: WordPress

1. **Remedies:**

* Upgrade JetPack plugin to version 3.3.6 or later as provided by the official vendor.
* Ensure proper user role assignments to minimize exposure (limit author-level access).
* Apply file upload validation mechanisms at the application and server level.

1. **Recommendations:**

* Patch JetPack plugin immediately to prevent exploitation.
* Monitor server logs for any suspicious upload or deletion activity.
* Conduct regular vulnerability assessments across all plugins.
* Use a Web Application Firewall (WAF) to detect and block suspicious file uploads.
* Limit privileges for lower-tier users (e.g., authors) to reduce exposure.

1. **References:**

* JetPack Critical Security Update – Official Advisory
* WPScan Vulnerability Report
* NVD CVE Entry - CVE-2023-2996