**Vulnerability Report**

**Name:** Prasad Jadhav

**Vulnerability Title:** Apache Tomcat AJP Connector Request Injection (Ghostcat)  
**Plugin ID:** 134862  
**CVE ID:** CVE-2020-1938, CVE-2020-1745  
**Host Scanned:** 192.168.1.88 (Metasploitable 1)  
**Tool Used:** Tenable Nessus Professional  
**Scan Date:** April 28, 2025

**1. Description:** A critical vulnerability exists in the Apache Tomcat AJP (Apache JServ Protocol) connector, known as **Ghostcat**, which allows unauthenticated attackers to exploit improperly handled AJP requests. If the AJP port is exposed (commonly 8009), an attacker can access internal files such as /WEB-INF/web.xml. In cases where file uploads are enabled, this vulnerability may be used to upload malicious JSP files and achieve **Remote Code Execution (RCE)**.

**2. Risk Summary:**

* **Risk Factor:** Critical
* **CVSS v3.0 Base Score:** 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
* **Attack Vector:** Network
* **Impact:**
  + Arbitrary file read
  + Local file inclusion
  + Possible remote code execution
* **Exploitable Remotely:** Yes
* **Authentication Required:** No

**3. Affected Software/Services:**

* **Software:** Apache Tomcat
* **Versions Affected:**
  + 9.0.0.M1 to 9.0.30
  + 8.5.0 to 8.5.50
  + 7.0.0 to 7.0.99
* **Default Vulnerable Port:** 8009 (AJP)

**4. Remedies:**

* Upgrade to **Apache Tomcat 9.0.31**, **8.5.51**, or **7.0.100**, or later versions as applicable.
* If AJP is not required, **disable the AJP connector** by commenting it out in server.xml.
* If AJP is needed:
  + Restrict access using a firewall or bind it to localhost only.
  + Enable the secretRequired="true" attribute and configure a secure secret.

**5. Recommendations:**

* Perform a complete Tomcat version upgrade if running an affected version.
* Use a firewall to **block public access** to port 8009.
* Regularly audit Tomcat’s server configuration and restrict exposed services.
* Monitor logs for suspicious access to sensitive files like /WEB-INF/web.xml.
* Ensure file uploads are strictly validated and do not allow executable code to be stored.

**6. References:**

* NVD - CVE-2020-1938
* Red Hat Advisory - CVE-2020-1745
* Apache Tomcat Official Security Page
* Tenable Plugin 134862 - Ghostcat