**Vulnerability Report**

**Name:** Prasad Jadhav

**Vulnerability Title:** Shellshock - Bash Remote Code Execution  
**Plugin ID:** 77823  
**CVE ID:** CVE-2014-6271  
**Host Scanned:** 192.168.1.79 (Metasploitable 2 VM)  
**Tool Used:** Tenable Nessus Professional  
**Scan Date:** 28 April 2025

1. **Description:** Shellshock is a vulnerability in the GNU Bash shell that allows attackers to execute arbitrary code by crafting malicious environment variables. This flaw arises when Bash incorrectly executes trailing code in function definitions passed via environment variables. If exploited, it can result in **unauthenticated remote code execution** on the affected system.
2. **Risk Summary**

* **Risk Factor:** Critical
* **CVSS v3.0 Base Score:** 9.8
* **Attack Vector:** Network
* **Impact:** Complete system compromise
* **Exploitable Remotely:** Yes
* **Authentication Required:** No

1. **Affected Software/Services:**

* **Bash version:** Vulnerable version on Metasploitable 2 (Ubuntu 8.04, Bash < 4.3)
* **Affected Service Port:** TCP/22 (SSH)

1. **Remedies:** Update Bash to a patched version.  
   On Ubuntu/Debian systems, run:

* sudo apt-get update
* sudo apt-get install --only-upgrade bash

1. **Recommendations:**

* Immediately patch the vulnerable Bash version.
* Disable unnecessary services (e.g., CGI scripts using Bash).
* Monitor logs for suspicious activity related to environment variable exploitation.
* Restrict external access to services like SSH using firewalls or VPNs.

1. **References:**

* National Vulnerability Database. CVE-2014-6271 Detail. NIST.
* Common Vulnerabilities and Exposures (CVE). CVE-2014-6271.
* Tenable Nessus Plugin ID 77823: Bash Shellshock Vulnerability (CVE-2014-6271).
* Ubuntu Security Notice USN-2362-1: Bash Vulnerability.
* Red Hat Security Blog. Shellshock: How to protect your systems.
* CERT Coordination Center (CERT/CC). Shellshock Vulnerability in Bash.