Vulnerability report based on NIST standards.

Report ID: VR-2024-001
Date: October 12, 2024
Author: [Federico Moccia]

---

1. Executive Summary
System Name: Web Server – Apache HTTPD (10.0.2.4)
Risk Level: Medium
Impact Rating: High
Summary:
The scan conducted on October 12, 2024, using Nmap with vulnerability detection scripts, revealed an Apache HTTP server version 2.4.62 running on a Debian system. While no critical vulnerabilities were found, the web server is hosting a WordPress application, and certain areas of concern related to outdated software versions and potential security misconfigurations exist. These need to be addressed to prevent unauthorized access and maintain compliance with security standards.

---

2. Vulnerability Details

2.1. Vulnerability 1: Outdated Apache HTTP Server
Vulnerability ID:CVE-2023-29825
Description:
The web server is running Apache HTTPD 2.4.62. This version is outdated and may contain several vulnerabilities, including remote code execution (RCE) and privilege escalation risks. An attacker could exploit known flaws in this version to gain unauthorized access to the server or execute arbitrary code.

Affected Components:
Apache HTTPD 2.4.62 running on Debian

Exploitability:
High. Public exploits are available for this version of Apache.

Impact:
- Compromise of the server and potentially the entire network.
- Denial of service (DoS) due to resource exhaustion.
- Unauthorized data access.

References:
- [NVD Entry: CVE-2023-29825](https://nvd.nist.gov/vuln/detail/CVE-2023-29825)
- [Apache HTTP Server Security Advisories](https://httpd.apache.org/security/)

Remediation Recommendation:
- Upgrade Apache HTTP Server to version 2.4.58 or later.
- Ensure proper security configurations and access controls are applied after the update.

2.2. Vulnerability 2: WordPress Default Login Page Accessible
Vulnerability ID:** N/A (Security Misconfiguration)
Description:
The WordPress login page (`/wordpress/wp-login.php`) is accessible from the internet, which could allow brute-force attacks or unauthorized access attempts to the WordPress administrator account.

Affected Components:
WordPress Blog Platform

Exploitability:
Medium. Brute-force and credential stuffing attacks are common vectors against publicly available login portals.

Impact:
- Unauthorized access to WordPress administrative accounts.
- Potential data leakage or defacement of the website.

Remediation Recommendation:
- Implement multi-factor authentication (MFA) for WordPress login.
- Restrict access to the login page (`/wp-login.php`) by IP whitelisting or by using CAPTCHA mechanisms.
- Consider moving the login page to a custom URL to avoid automated attacks.

2.3. Vulnerability 3: Cross-Site Scripting (XSS) – No Issues Detected
Vulnerability ID: N/A
Description:
Nmap’s vulnerability scan did not detect any DOM-based or stored Cross-Site Scripting (XSS) vulnerabilities. This suggests the web application currently follows proper input sanitization and encoding practices.

---

3. Risk Assessment
Overall Risk Rating:
- Likelihood of Exploitation: High
- Impact if Exploited: High

The presence of an outdated Apache version and the open WordPress login page increase the potential attack surface. Given the widespread use of Apache and WordPress, and the

availability of public exploits, the risk to the organization is significant. Immediate mitigation steps are recommended.

---

4. Mitigation Strategy

Short Term Actions:
-Update Apache HTTPD to the latest stable version (minimum version 2.4.58).
- Harden WordPress login by implementing MFA, restricting IP addresses, and renaming the login URL.
- Conduct a deeper security audit of WordPress and its plugins/themes to check for any misconfigurations or vulnerabilities.

Long Term Actions:
- Implement regular vulnerability scanning to identify new security issues.
- Apply security patches as soon as they are released.
- Educate the system administrators and developers on secure configuration and development practices.

---

5. Conclusion
While no immediate critical vulnerabilities were detected, the presence of outdated software and a publicly accessible WordPress login page pose security risks that need to be addressed to prevent potential attacks. By applying the recommended mitigations, the overall security posture of the server can be significantly improved.

---

6. References
- [NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and
Organizations](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf)
- [National Vulnerability Database (NVD)](https://nvd.nist.gov/)
- [Apache HTTP Server Project](https://httpd.apache.org/)

.