1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain `wwh-api.channel-warranty-warehouse-prod-vpn2.` using a Basic scan type. The analysis commenced on April 12th at 13:00 and concluded in **00h:09m:37s**. The tracking ID for this assessment is **0152c35191a7**. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, following OWASP and OSCP methodologies.

1.2 Key Security Issues

Title	Risk
SSL/TLS Protocols Security Assessment	High
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium

1.3 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **1 High-risk**, **2 Medium-risk**, **3 Low-risk**, and **12 informational**. The most critical finding is the use of deprecated and vulnerable SSL/TLS protocols (TLS 1.0 and 1.1) on two endpoints, posing significant security risks such as susceptibility to BEAST attacks. Additionally, the Nmap port scan revealed an open HTTP port (**80**) without encryption, necessitating verification for HTTPS redirection or HSTS implementation. The subdomain naming assessment highlighted potentially sensitive endpoints, indicating a need for enhanced security measures. Overall, **100%** of servers are located in the USA, with no High-risk geographic locations detected. Immediate actions should focus on upgrading SSL/TLS protocols and securing exposed ports to mitigate potential threats.

1.4 SSL/TLS Protocols Security Assessment

1.4.1 Description

The assessment revealed that two endpoints are utilizing deprecated SSL/TLS protocols, specifically TLS 1.0 and TLS 1.1. These protocols are vulnerable to known attacks such as BEAST and lack modern cryptographic algorithms, posing a critical security risk.

1.4.2 Affected Assets

- **Endpoints using TLS 1.0: 2**
- **Endpoints using TLS 1.1: 2**
- **Endpoints using TLS 1.2: 2**
- **Endpoints with TLS 1.3 support: 0**
- **Endpoints with SSLv3: 0**

1.4.3 Recommendations

Immediate upgrade of all endpoints to support TLS 1.2 as a minimum standard, with a strong recommendation to implement TLS 1.3 for enhanced security and performance. Ensure all deprecated protocols are disabled to prevent exploitation.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING

1.5 Nmap Port Scan Results Analysis

1.5.1 Description

The Nmap port scan identified an open HTTP port (**80**) on the IP address **18.233.172.20** without encryption, which could expose sensitive data if not properly secured through HTTPS redirection or HSTS implementation.

1.5.2 Affected Assets

- **IP Address: 18.233.172.20**
- **Open Ports: 80/tcp** (http), **443/tcp** (ssl/https)

1.5.3 Recommendations

Verify that HTTP traffic is redirected to HTTPS and that HSTS is enabled to enforce secure connections. Regularly monitor open ports and services to ensure they are appropriately secured.

1.6 Subdomain Naming Security Assessment

1.6.1 Description

The analysis identified a sensitive subdomain that may provide access to administrative interfaces or internal systems, posing a Medium security risk due to potential exposure of critical systems and sensitive data.

1.6.2 Affected Assets

- **Subdomain:** wwh-api.channel-warranty-warehouse-prod-vpn2.us.e06.c01.johndeerecloud.com

1.6.3 Recommendations

Implement strict access controls and monitoring on sensitive subdomains to prevent unauthorized access. Regularly review subdomain configurations to ensure they do not expose unnecessary information or services.

1.7 General Recommendations

To enhance overall security posture, it is recommended to:

- Conduct regular security assessments to identify and remediate vulnerabilities promptly.
- Implement a robust patch management process to ensure all systems are up-to-date with the latest security patches.
- Educate employees on security best practices and conduct regular training sessions to raise awareness about potential threats.
- Establish a comprehensive incident response plan to quickly address any security breaches or incidents.

By addressing these vulnerabilities and following the recommended actions, the organization can significantly reduce its risk exposure and improve its security resilience.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING