Pinewheel.ai Security Assessment

Initial Report: February 22, 2025
First Revision: February 24, 2025
For: Pinewheel.ai

Confidentiality Statement

All information contained in this document is provided in confidence for the sole purpose of security assessment and shall not be disclosed wholly or in part to any third party without prior written permission. These obligations shall not apply to publicly available information.

Disclaimer

This document is provided for information purposes only. No responsibility is accepted for errors or omissions. This document is provided without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose, and non-infringement. The findings in this document are based on the scope of testing performed and do not guarantee complete security.

1. Overview

Scope

At the start of the engagement, the security team worked with Pinewheel.ai to define the target and establish the limits of the test. The assessment followed a **black-box** penetration testing methodology, where testing was conducted externally without prior access to system internals.

Target Environment:-

Application Name	**Pinewheel.ai**
Codebase	Web Application
Hosting	AWS CloudFront
OS Detected	Ubuntu 16.04 Linux Kernel 4.4

Audit Summary:-

Delivery Date	**February 22,2025**
Method Of Audit	Dynamic Testing,Network Scanning
Consultants Engaged	1
Timeline	February 20-22,2025

Vulnerability Summary:-

Severity Level	**Count**
Critical	**1**
High	**2**
Medium	**2**
Low	**1**
Informational	**1**

2. Executive Summary

Pinewheel.ai engaged the security team to conduct a **penetration test** to identify potential security risks. The assessment found **multiple vulnerabilities**, including:

1. **An outdated operating system (Critical)** – Potential for **privilege escalation and remote code execution (RCE)**.
2. **CloudFront WAF misconfiguration (High)** – Risk of security bypass and **unauthorized access**.
3. **Potential SSRF via API endpoints (High)** – Possible **server-side request forgery**.
4. **Exposed security headers and misconfigurations (Medium)** – Allowing fingerprinting and targeted attacks.
5. **Exposed internal documentation (Medium)** – Increasing attack surface.

These findings highlight the need for **immediate security patches**, **proper authentication mechanisms**, and **enhanced API request validation** to mitigate risks.

3. Findings

ID: PINE-01 - Outdated Operating System and Privilege Escalation Risks

1. **Severity: Critical**
2. **Description:** The target system runs **Ubuntu 16.04 with Linux Kernel 4.4**, which has reached **End-of-Life (EOL)**, exposing it to **publicly known CVEs**.
3. **Potential CVEs:**
    a. **CVE-2022-0492:** Container escape via control groups.
    b. **CVE-2023-32233:** Netfilter use-after-free vulnerability.
    c. **CVE-2022-0847:** Dirty Pipe privilege escalation exploit.
    d. **CVE-2022-32250:** Stack buffer overflow leading to remote code execution.
4. **Recommendation: Upgrade to Ubuntu 20.04 or later** and apply security patches.

ID: PINE-02 - CloudFront WAF Bypass via Header Manipulation

1. **Severity: High**
2. **Description:** CloudFront's **misconfiguration** allows an attacker to **manipulate HTTP headers** (`X-Forwarded-For`, `X-Originating-IP`) to bypass security controls.
3. **Impact:** Unauthorized access to internal APIs and sensitive areas of the application.
4. **Recommendation:** Implement **strict WAF rules** to block unauthorized requests.

ID: PINE-03 - Potential SSRF (Server-Side Request Forgery) via API Endpoints

1. **Severity: High**
2. **Vulnerable Endpoint:** `/api/og?url=`
3. **Description:** The API processes **user-supplied URLs**, which could be exploited to **request internal resources**.
4. **Impact:** Attackers might **access internal metadata** or **internal services**.
5. **Recommendation:** Implement **URL allowlisting** and **strict validation**.

ID: PINE-04 - Web Application Misconfigurations & Information Disclosure

1. **Severity: Medium**
2. **Description:** Headers like `X-Powered-By` and `Server` are exposed, revealing framework details.
3. **Impact:** Attackers can **fingerprint the stack** and **craft targeted exploits**.
4. **Recommendation: Remove unnecessary headers** to prevent information leakage.

ID: PINE-05 - Exposed Internal Documentation

1. **Severity: Medium**
2. **Description:** `docs.pinewheel.ai` was found **publicly accessible without authentication**.
3. **Impact:** Attackers could use this **for reconnaissance**.
4. **Recommendation:** Restrict access to **authorized users only**.

ID: PINE-06 - Uses of Insecure Protocols

1. **Severity: Low**
2. **Description:** Communication between the application and backend **is not fully encrypted**.
3. **Impact:** Potential **man-in-the-middle (MITM) attacks**.
4. **Recommendation:** Enforce **TLS 1.2 or higher** for all communications.

4. Risk Assessment

Risk Level	CVSS Score	Impact
Critical	9.0-10.0	Full system compromise, large-scale data breach
High	7.0-8.9	Privilege escalation, significant data loss or downtime
Medium	4.0-6.9	Limited access, affecting operations and compliance
Low	0.1-3.9	Minimal impact, mostly affecting non-critical functions
Informational	0.0	Discloses information but not exploitable directly

5. Recommendations

1. **Upgrade the OS (Critical)** – Migrate to **Ubuntu 20.04 or later**.
2. **Harden CloudFront security (High)** – Implement **strict WAF rules**.
3. **Remove security headers (Medium)** – Prevent stack fingerprinting.
4. **Fix API validation (High)** – Prevent **SSRF attacks**.
5. **Restrict access to documentation (Medium)** – Secure internal resources.
6. **Enforce TLS (Low)** – Mitigate **MITM attacks**.