
Third-Party Penetration Testing Attestation

We periodically engage **independent third-party security auditors** during major release cycles (e.g., **v4.0.0**) to validate the security, stability, and integrity of the **KiviCare Telemed Addon**.

1. Testing Methodology
Our testing partners conduct both **Black-box** and **Gray-box** penetration testing. The assessments specifically focus on the interaction between **WordPress user role permissions** and **Zoom API authorization flows**, which represent critical security boundaries within the application.

2. Target Scope
The most recent penetration test concentrated on high-risk attack vectors identified within the codebase, including:

- **OAuth State Validation:**
  Validation of the `handleZoomCallback` method in `KCTZoomController.php` to ensure robust **Cross-Site Request Forgery (CSRF)** protection and to prevent unauthorized takeover of a Doctor's Zoom integration.
- **Webhook Integrity:**
  Attempts to bypass **HMAC (`hash_hmac`) signature verification** within `KCTZoom::handle_webhook` to assess the risk of spoofed or tampered meeting status events.
- **IDOR (Insecure Direct Object References):**
  Verification that a Doctor cannot access, query, modify, or disconnect the Zoom configuration of another Doctor via the `/doctor-config` REST API endpoint.

3. Remediation Policy
Any **critical or high-severity vulnerabilities** identified during third-party assessments are **remediated immediately** and verified prior to production release deployment.
