Vulnerability Disclosure Program (VDP) HackedAlert

1. Introduction

At HackedAlert, the security of our users and the integrity of our systems are our top priority.

We value the work of the cybersecurity community and believe that collaboration with independent researchers is essential to strengthening our defenses.

This document outlines the policies of our VDP program and establishes the guidelines for responsible vulnerability disclosure.

2. Scope (In-Scope)

Only reports regarding the following assets will be accepted:

- **Domains**: hackedalert.com, leymarcodeciberseguridad.cl, wl-inc.cl
- **Subdomains**: *.hackedalert.com, *.leymarcodeciberseguridad.cl, *.wl-inc.cl

3. Exclusions (Out-of-Scope)

The following are strictly excluded from this program:

- Social engineering, phishing, or physical attacks against employees or facilities.
- Denial of Service (DoS/DDoS) attacks.
- Third-party systems (e.g., cloud providers, third-party libraries without proprietary integration).
- Vulnerabilities requiring physical access or already compromised user privileges.
- Vulnerabilities such as Text Spoofing, HTML Injection, CSRF on logout/login, outdated technology versions without impact demonstration, and any other type of vulnerability that can be categorized as low severity or informational due to a lack of impact.
- Vulnerabilities such as Rate Limit Bypasses are considered low severity unless they involve a medium, high, or critical impact; another clear example is user enumeration and brute-force attacks. Evading a security system by itself is not considered a vulnerability in our VDP program.

4. Vulnerabilities in Scope

While no system is completely secure and may present various types of vulnerabilities, we are particularly interested in the discovery and reporting of the following types of bugs:

- **Severity**: Medium, high, and critical severity vulnerabilities.
- **Impact**: Vulnerabilities with a technically verifiable impact on user data within the platform.
- **Vulnerability Types**: Remote Code Execution (RCE), Server-Side Request Forgery (SSRF), Code Injection and Command Injection, Arbitrary JavaScript Execution (r-XSS, d-XSS, and s-XSS), Vertical and Horizontal Privilege Escalation, IDOR, CRLF Injection, HTTP Request Smuggling, Insecure Deserialization, SQL Injection, Cache Poisoning/Deception, among other vulnerabilities with a demonstrated medium, high, or critical impact.
- **Bug Chaining**: The chaining of multiple low-severity vulnerabilities that result in an overall medium, high, or critical impact.

4. Pautas de "Safe Harbor" (Puerto Seguro)

Si usted actúa de buena fé y cumple con esta política, HackedAlert:

1. No iniciará acciones legales contra usted.
2. Trabajará con usted para comprender y resolver el problema de manera rápida.
3. No notificará a autoridades legales, salvo requerimiento policial o judicial vinculante.

5. Reporting Instructions

To report a vulnerability, please send an email to contacto@wl-inc.cl with the following information:

- **Report format**: Markdown file (*.md).
- **Reproduction steps**: Exact steps to reproduce the vulnerability.
- **Impact description**: A detailed description of the impact and its categorization using CVSS 4.0.
- **Proof of Concept (PoC)**: Screenshots, logs, or scripts (please ensure you redact or avoid using real user data).
- **Contact information**: Name and contact details of the researcher.
- **File format**: Preferably, the report should be packaged in a .zip or .rar file.

6. What to Expect from Our Program

When collaborating with us, you can expect transparent and professional communication throughout the lifecycle of your report:

- **Expectation Management**: Our security team will evaluate each report individually. Eligibility will be based on technical relevance, the clarity of the Proof of Concept (PoC), and the criticality of the reported risk.
- **Triage Process**: Once your report is received, we will conduct an internal validation to confirm the vulnerability. During this time, we may contact you to request technical clarifications or additional testing environments.
- **Remediation Feedback**: Once a legitimate, in-scope vulnerability is confirmed and validated, we will keep you informed about the progress of the patch or the mitigation measures implemented.
- **Recognition**: We value the effort of our researchers. If your report contributes significantly to our security, we will publicly acknowledge your contribution through our "Hall of Fame," provide a Letter of Appreciation, and/or offer a Limited Edition Challenge Coin (subject to availability; these are generally of limited access).
- **Safe Harbor (No-Retaliation Commitment)**: We are committed to maintaining a collaborative environment. As long as you respect the guidelines of this policy, we guarantee that we will not pursue legal action or retaliation against your good-faith efforts to improve our security posture.

7. Rules of Engagement

- **Privacy**: Do not access, modify, or download customer data. If you encounter personal data, stop immediately and notify us.
- **Integrity**: Do not perform tests that may degrade the availability of the service.
- **Disclosure**: You agree not to publicly disclose any vulnerability for a period of 90 days from the date it is reported, or until HackedAlert has confirmed the resolution and explicitly authorized publication (90-day confidentiality period).

8. Evaluation Process

- **Acknowledgment of Receipt**: We will respond within a maximum of 3 business days.
- **Evaluation**: We will classify the severity according to CVSS 4.0 standards.
- **Remediation**: We will work on the patch based on the criticality identified.

9. Contact

For any questions or requirements, you may contact our team using the following email address: contacto@wl-inc.cl.

Santiago, Chile, May 26, 2026.