Vulnerability Disclosure Program (VDP) HackedAlert

1. Introducción

En HackedAlert, la seguridad de nuestros usuarios y la integridad de nuestros sistemas son prioridad.

Valoramos la labor de la comunidad de ciberseguridad y creemos que la colaboración con investigadores independientes es esencial para fortalecer nuestras defensas.

El presente documento representa las políticas de nuestro programa VDP, y establece los lineamientos para la notificación responsable de vulnerabilidades.

2. Ámbito de Aplicación (In-Scope)

Solo se aceptarán reportes sobre los siguientes activos:

- Dominios: hackedalert.com, leymarcodeciberseguridad.cl, wl-inc.cl
- Subdominios: *.hackedalert.com, *.leymarcodeciberseguridad.cl, *.wl-inc.cl

3. Exclusiones (Out-of-Scope)

Quedan estrictamente excluidos de este programa:

- Ingeniería social, phishing o ataques físicos contra empleados o instalaciones.
- Ataques de Denegación de Servicio (DoS/DDoS).
- Sistemas de terceros (ej. proveedores de nube, librerías de terceros sin integración propietaria).
- Vulnerabilidades que requieran acceso físico o privilegios de usuario ya comprometidos.
- Vulnerabilidades como Text Spoofing, HTML Injection, CSRF en logout/login, versiones de tecnologías obsoletas sin demostración del impacto, y cualquier otro tipo de vulnerabilidad que pueda ser categorizada como severidad baja o informacional producto de la ausencia de impacto.
- Vulnerabilidades como Bypass de Rate Limit son consideradas de baja severidad, si no involucran un impacto de severidad media, alta o crítica; otro ejemplo claro, es la enumeración de usuarios y los ataques de fuerza bruta; evadir un sistema de seguridad por sí mismo, no es considerado una vulnerabilidad en nuestro programa VDP.

4. Vulnerabilidades en Alcance (In-Scope)

Si bien es cierto ningún sistema es completamente seguro, y puede presentar diferentes tipos de vulnerabilidades, estamos particularmente interesados en el hallazgo y reportería de los tipos de bugs:

- Severidad: vulnerabilidades de severidad media, alta y crítica.
- Impacto: vulnerabilidades con impacto técnicamente comprobable, sobre datos de usuarios de la plataforma.
- Vulnerabilidades: Remote Code Execution (RCE), Server-Side Request Forgery (SSRF), Code Injection y Command Injection, Ejecución arbitraria de JavaScript (r-XSS, d-XSS y s-XSS), Escalamiento de Privilegios Vertical y Horizontal, IDOR, CRLF Injection, HTTP Request Smuggling, Insecure Deserialization, SQL Injection, Cache Poisoning/Deception, entre otras vulnerabilidades con demostración de impacto con severidad media, alta o crítica.
- Bug Chaining: el encadenamiento de múltiples vulnerabilidades de severidad baja que derivan en un impacto de severidad media, alta o crítica.

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. Instrucciones para el Reporte

Para reportar una vulnerabilidad, envíe un correo a contacto@wl-inc.cl con la siguiente información:

- Reporte en formato de texto markdown (*.md)
- Pasos exactos para reproducir la vulnerabilidad.
- Descripción del impacto y su categorización usando CVSS 4.0
- Prueba de concepto (PoC): Capturas de pantalla, logs o scripts (evite datos reales de usuarios).
- Información de contacto: Nombre y datos de contacto del investigador.
- De preferencia, el reporte empaquetado en formato zip o rar

6. ¿Qué esperar de nuestro Programa?

Al colaborar con nosotros, usted puede esperar una comunicación transparente y profesional durante todo el ciclo de vida de su reporte:

- Gestión de Expectativas: Nuestro equipo de seguridad evaluará cada informe de forma individual. La elegibilidad de un reporte se basará en la relevancia técnica, la claridad de la PoC y la criticidad del riesgo reportado.
- Proceso de Triaje: Una vez recibido su reporte, realizaremos una validación interna para confirmar la vulnerabilidad. Durante este tiempo, es posible que le contactemos para solicitar aclaraciones técnicas o entornos de prueba adicionales.
- Feedback sobre la Remediación: Una vez confirmada y validada una vulnerabilidad legítima (dentro del alcance), le mantendremos informado sobre el progreso del parche o las medidas de mitigación implementadas.
- Reconocimiento: Valoramos el esfuerzo de los investigadores. Si su reporte contribuye significativamente a nuestra seguridad, reconoceremos públicamente su aporte, a través de nuestro "Hall of Fame", la entrega de una Carta de Agradecimiento, y/o una Challenge Coin de Edición Limitada (sujetas a disponibilidad, generalmente, de acceso limitado).
- Compromiso de No-Retaliación: Nuestro compromiso es mantener un entorno de colaboración. Mientras usted respete los lineamientos de esta política, garantizamos que no tomaremos represalias ni acciones legales contra sus esfuerzos de buena fe orientados a mejorar nuestra postura de seguridad.

7. Reglas de Compromiso

- Privacidad: No acceda, modifique ni descargue datos de clientes. Si encuentra datos personales, deténgase inmediatamente y notifique.
- Integridad: No realice pruebas que puedan degradar la disponibilidad del servicio.
- Divulgación: Usted se compromete a no hacer pública ninguna vulnerabilidad por el plazo de 90 días desde que es reportada, o hasta que HackedAlert haya confirmado la resolución y autorizado explícitamente la publicación (periodo de confidencialidad de 90 días).

8. Proceso de Evaluación

- Acuse de recibo: Responderemos en un plazo máximo de 3 días hábiles.
- Evaluación: Clasificaremos la severidad bajo estándares CVSS 4.0.
- Remediación: Trabajaremos en el parche según la criticidad hallada.

9. Contacto

Frente a cualquier duda o requerimiento, puede tomar contacto con nuestro equipo utilizando el siguiente correo electrónico: contacto@wl-inc.cl.

Santiago de Chile, 26 de Mayo de 2026.