Divulgación responsable de posibles vulnerabilidades

En PATAGONIA BIONERGÍA (Grupo Viterra), la seguridad global de nuestros sistemas online es nuestra prioridad. A pesar del constante esfuerzo que invertimos en la seguridad de nuestros sistemas, no significa que nuestros sistemas estén exentos de eventuales vulnerabilidades en materia de seguridad. Si usted descubre un posible riesgo en materia de seguridad, por favor infórmenos a fin de tomar las acciones necesarias.

Como proceder:

1. Ingrese su hallazgo a través del siguiente link: https://app.zerocopter.com/en/cvd/623850a7-c366-4da7-849c-b011a6c6aa12
1. Reporte la potencial vulnerabilidad tan pronto como le sea posible a fin de minimizar el riesgo de una falla de seguridad.
2. Reporte el riesgo de manera confidencial, a fin de evitar que otros terceros logren acceder a dicha información. Por ejemplo, no comparta el reporte ni lo publique de ninguna manera en portales web de acceso público.
3. Provea la información de manera detallada para que podamos resolver el problema. Por lo general, será suficiente con suministrar la dirección IP o la URL de los sistemas afectados, y una breve descripción de la eventual vulnerabilidad. Por favor tener en cuenta que las vulnerabilidades más complejas requerirán mayor explicación.
4. Siga de cerca nuestras instrucciones después de haber enviado el hallazgo.

Acciones prohibidas al momento de realizar la divulgación:

1. No incumplir con ninguna ley o regulación aplicable al momento de investigar y reportar una vulnerabilidad o problema.
2. No revelar la vulnerabilidad o el problema bajo ningún concepto antes de que sea resuelto.
3. No crear un Backdoor en nuestros sistemas de información online con la intención de usarla para demostrar la vulnerabilidad. Proceder de dicha manera podría significar en un prejuicio adicional y crear un riesgo de seguridad innecesario.
4. No utilizar la vulnerabilidad más de lo necesario para establecer su existencia.
5. No abusar o sacar ventaja de la vulnerabilidad; por ejemplo, mediante la descarga, copia, modificación, o eliminación de datos en el sistema. Por ejemplo, en vez de descargar información para dimensionar la vulnerabilidad, usted puede hacer una lista de directorios del sistema.
6. No interrumpir, hacer cambios o ajustes en el sistema.
7. No compartir el acceso a los sistemas con otros ni ingresar reiteradamente.
8. No realizar ataques de fuerza bruta, ni ataques a la seguridad física, a la ingeniería social, denegación de servicio distribuido, spam, o aplicaciones de terceros para ganas acceso al sistema.
9. No solicitar ningún tipo de recompensa por reportar la potencial vulnerabilidad.

Nuestro compromiso:

- Le responderemos su reporte tan pronto como nos sea razonablemente posible.
- Está permitido reportar bajo un seudónimo o de manera anónima.
- Lo mantendremos informado, en lo posible, respecto al progreso de la solución del problema.
- Al momento de publicar la información relacionada con la vulnerabilidad reportada, usted será mencionado como colaborador y artífice del descubrimiento de dicha vulnerabilidad (a menos que usted prefiera lo contrario).

Nos comprometemos a no iniciar acciones legales si al momento de reportar las posibles vulnerabilidades se siguen estrictamente los lineamientos aquí expuestos, siempre en cumplimiento de la normativa aplicable.