Política de Divulgación de Vulnerabilidades

Última Modificación: 26 de abril de 2024

Esta Política de Divulgación de Vulnerabilidades forma parte del compromiso de Ubicquia, Inc. ("**Ubicquia**" o la "**Compañía**") hacia la seguridad de sus clientes y la comunidad de Internet en general. Ubicquia valora las contribuciones de los investigadores de seguridad y los usuarios que toman el tiempo y hacen el esfuerzo para reportar vulnerabilidades de seguridad de acuerdo con esta política. Ubicquia actuará de buena fe para resolver las vulnerabilidades reportadas de acuerdo con esta política.

1. Introducción

Este documento describe la política de divulgación de vulnerabilidades de Ubicquia. Esta política tiene como objetivo garantizar la seguridad e integridad de los productos y servicios de la Compañía, y a la vez fomentar la colaboración con la comunidad de investigación en seguridad. Ubicquia está comprometida con el manejo responsable de vulnerabilidades de acuerdo con esta política. Esta política se aplica a cualquier vulnerabilidad que está siendo considerada para ser reportada a la Compañía y recomendamos leer esta política antes de reportar una vulnerabilidad.

2. Notificación de Vulnerabilidades

Se les anima a los investigadores de seguridad o usuarios que descubran vulnerabilidades en los productos o sistemas de la Compañía a informar de ellas a través del correo electrónico: vulnerability@ubicquia.com.

En el informe, por favor proporcione los detalles a continuación:
* El sitio web, IP o página donde se observa la vulnerabilidad.
* Una breve descripción del tipo de vulnerabilidad, por ejemplo, "vulnerabilidad XSS".
* Pasos para reproducirla. Deben ser una prueba de concepto benigna y no destructiva. Esto ayuda a garantizar que el informe se pueda clasificar con rapidez y precisión. También reduce la probabilidad de informes duplicados, o la explotación maliciosa de algunas vulnerabilidades, como la toma de sub-dominios.

3. Compromisos

La Compañía se compromete a actuar oportunamente ante las vulnerabilidades reveladas. Tras recibir un informe, evaluaremos el problema y tomaremos las medidas necesarias para solucionarlo.

La Compañía hará un esfuerzo comercialmente razonable para acusar recibo de los informes de vulnerabilidad en un plazo de 5 días laborables y para clasificar dichos informes en un plazo de 10 días laborables. Cualquier acuse de recibo por escrito de la Compañía incluirá una evaluación inicial del informe y los pasos siguientes.

La prioridad de la remediación se evalúa teniendo en cuenta el impacto, la gravedad y explotación de la complejidad. Priorizamos el tratamiento de las vulnerabilidades críticas para garantizar que se abordan con la debida urgencia.

Ubicquia proporcionará actualizaciones de estado regulares de conformidad con las obligaciones contractuales existentes. Como mínimo, la Compañía proporcionará actualizaciones de estado al menos cada dos semanas hasta que se resuelva el problema.

4. Proceso de Resolución

Investigación y Validación: Tras la recepción de un informe de vulnerabilidad, el equipo de seguridad de Ubicquia llevará a cabo una investigación inicial para validar el problema.

Remediación: La Compañía desarrollará un plan de remediación para abordar la vulnerabilidad. Esto puede incluir soluciones temporales, parches o actualizaciones de nuestros productos o sistemas.

5. Orientación

Usted **NO** debe:

* Infringir ninguna ley o normativa aplicable.
* Recuperar, acceder o modificar ningún dato de los sistemas o servicios de la Compañía.
* Utilizar herramientas de exploración invasivas o destructivas de alta intensidad para encontrar vulnerabilidades.
* Intentar o notificar cualquier forma de denegación de servicio, por ejemplo, saturar un servicio con un elevado volumen de solicitudes.
* Interrumpir los servicios o sistemas de la Compañía.
* Presentar informes que detallen vulnerabilidades no explotables, o informes que indiquen que los servicios no se ajustan plenamente a las “mejores prácticas”, por ejemplo, falta de cabeceras de seguridad.
* Presentar informes que detallen deficiencias en la configuración de TLS, por ejemplo, compatibilidad con conjuntos de cifrado “débiles” o la presencia de suporte TLS 1.0.
* Comunicar cualquier vulnerabilidad o detalles asociados por medios distintos a los descritos en los datos de contacto.
* Realizar ingeniería social, “phishing” la Compañía.
* Exigir una compensación económica para revelar cualquier vulnerabilidad.

Usted debe:

* Cumplir siempre con las normas de protección de datos y no debe violar la privacidad de los usuarios, personal, contratistas, servicios o sistemas de la Compañía. Por ejemplo, no debe recuperar datos de nuestros sistemas.
* Si alguien recupera datos de nuestros sistemas por error, todos los datos recuperados deben ser borrados de forma segura inmediatamente después de su realización (estos datos no deben ser compartidos, redistribuidos).

6. Contacto

Para más información o para enviar un informe de vulnerabilidad, póngase en contacto con nosotros a través del correo electrónico vulnerability@ubicquia.com. Este método de contacto está asegurado para proteger la confidencialidad de la información compartida.

7. Legalidades

Esta política está diseñada para ser compatible con las buenas prácticas habituales en materia de divulgación de vulnerabilidades. No le da permiso para actuar de ninguna manera que sea incompatible con la ley, código ético, o que pueda causar que la Compañía o las organizaciones asociadas incumplan cualquier obligación legal.