[logotipo:] verisure

POLÍTICA DE DIVULGACIÓN RESPONSABLE DEL GRUPO

Abril de 2024

Introducción

Verisure se compromete a garantizar la seguridad de nuestros Productos, Sistemas y todos los datos de clientes, socios y empleados. Valoramos la colaboración con nuestra comunidad de usuarios e investigadores que pueden contribuir a la identificación de Vulnerabilidades de seguridad en nuestros Productos y Sistemas.

Esta Política establece un proceso para la divulgación responsable de Vulnerabilidades de seguridad, con el objetivo de facilitar una colaboración eficaz y una resolución rápida de los problemas de seguridad. Esta Política establece directrices para informar y gestionar las Vulnerabilidades de seguridad de forma responsable, de acuerdo con las normas de actuación que se indican a continuación, y se aplica a cualquier Vulnerabilidad de seguridad de la que se plantee informar a Verisure.

Le recomendamos que lea esta Política en su totalidad antes de informar sobre una posible Vulnerabilidad de seguridad.

Tenga en cuenta que Verisure no ofrece recompensas económicas por revelar Vulnerabilidades de seguridad.

Cómo informar de una vulnerabilidad

Verisure investiga todos los informes de Vulnerabilidades de seguridad que afectan a sus Productos y Servicios. Si cree que ha encontrado una Vulnerabilidad de seguridad en un Producto o Servicio de Verisure, envíe el informe de vulnerabilidad a través del siguiente formulario, proporcionando detalles suficientes para que podamos reproducir e investigar sus acciones. Es necesario rellenar correctamente todos los campos obligatorios y recuerde que, en virtud de esta Política, es esencial que mantenga la confidencialidad al informar de una Vulnerabilidad de seguridad. Le rogamos que no haga pública su investigación hasta que Verisure haya completado la investigación, haya resuelto o mitigado la Vulnerabilidad de seguridad y le haya concedido permiso para hacerlo.

Política de Divulgación Responsable del Grupo | Verisure

Siguientes pasos

Tras enviar su informe, Verisure notificará al denunciante que el informe se ha recibido correctamente y comenzará el análisis del mismo. Verisure podrá ponerse en contacto con el denunciante a través del portal web anónimo para recabar más información sobre el informe y mantenerle informado sobre el progreso hasta su cierre.

Nuestro proceso interno para abordar la Vulnerabilidad de seguridad comenzará por revisar el informe y determinar su impacto, gravedad y complejidad antes de poner en marcha medidas correctivas según corresponda.

Verisure se reserva el derecho a compartir el contenido del informe de Vulnerabilidad de seguridad presentado y cualquier hallazgo posterior con las partes pertinentes, pero no revelará los detalles asociados al denunciante.

Productos o servicios de terceros

Los productos, sistemas y datos que no sean propiedad de Verisure no están cubiertos por esta Política. Los denunciantes deben seguir las políticas de divulgación responsable proporcionadas por las respectivas terceras partes si desean realizar investigaciones o pruebas de estos sistemas.

Normas de actuación

Verisure valora los esfuerzos y las contribuciones de la comunidad de investigadores de seguridad y exige que se respeten las siguientes normas. Verisure no emprenderá acciones legales contra los denunciantes que descubran y revelen Vulnerabilidades de seguridad de buena fe y de acuerdo con esta Política.

El denunciante no debe:

- Incumplir ninguna ley o normativa aplicable.
- Introducir una nueva Vulnerabilidad de seguridad o intentar aprovecharse de una existente.
- Participar en ingeniería social o cometer ciberestafas con clientes o empleados.
- Exigir una compensación económica a cambio de la divulgación de una Vulnerabilidad de seguridad.
- Acceder a sistemas o datos más allá de lo necesario para identificar e informar de una Vulnerabilidad de seguridad.
- Manipular los dispositivos del sistema de alarma o los sistemas pertenecientes a clientes existentes, aunque sea el suyo propio.
- Modificar, copiar, compartir, corromper o afectar de cualquier otro modo a los datos procesados o almacenados en los Productos o sistemas de Verisure.
- Utilizar herramientas de escaneo de alta intensidad, invasivas o destructivas para encontrar Vulnerabilidades de seguridad, o realizar actividades disruptivas que incluyan, entre otras, ataques de fuerza bruta, ataques de denegación de servicio o ataques físicos contra las instalaciones o centros de datos de Verisure.
- Interrumpir las señales de alarma, las notificaciones o manipular físicamente su propio sistema de alarma de cualquier forma.
- Realizar pruebas o investigaciones con relación a servicios o sistemas de terceros que no pertenezcan a Verisure, como por ejemplo, infraestructuras externas de proveedores en la nube.
- Acceder a volúmenes de datos innecesarios, excesivos o significativos más allá de lo estrictamente necesario para descubrir y confirmar la Vulnerabilidad de seguridad.

El denunciante debe:

- Acceder a los datos y sistemas solo en la medida necesaria para confirmar la existencia de una Vulnerabilidad de seguridad.
- Detener las actividades de investigación o pruebas al confirmar la existencia de una Vulnerabilidad de seguridad, e informar de los hallazgos a Verisure sin demora.
- Eliminar de forma segura todos los datos obtenidos durante la investigación tan pronto como se haya informado de la Vulnerabilidad de seguridad y se haya recibido la confirmación de aceptación por parte de Verisure.
- Esperar la aprobación por escrito de Verisure antes de divulgar públicamente los detalles de la Vulnerabilidad de seguridad. Verisure también debe aprobar el contenido de la divulgación pública.

Qué no se debe notificar:

- Informes duplicados de Vulnerabilidades de seguridad.
- Informes que detallen las Vulnerabilidades de seguridad no explotables.
- Errores en la interfaz de usuario, en la experiencia del usuario o faltas de ortografía.
- Informes que indiquen que los Productos y Servicios no se ajustan plenamente a las “mejores prácticas”, como la falta de cabeceras de seguridad o el auto-XSS.

Verisure debe:

- Confirmar que ha recibido el informe de la Vulnerabilidad de seguridad en un plazo de 30 días a partir de la recepción del informe.
- Proporcionar actualizaciones de estado quincenales al denunciante desde la confirmación de recepción anterior hasta el cierre del informe de Vulnerabilidad de la seguridad.

- Comunicar por escrito su decisión sobre si el denunciante puede o no divulgar públicamente la Vulnerabilidad de seguridad. Si Verisure lo ha acordado previamente, Verisure deberá revisar el contenido de la divulgación pública antes de publicarla.

Definiciones

Vulnerabilidad de seguridad

Vulnerabilidades de seguridad específicas detectadas en los Productos o Servicios de Verisure que representan una debilidad hallada en los componentes de software o hardware que, al ser explotada, puede repercutir negativamente en la confidencialidad, integridad o disponibilidad de los datos o servicios de Verisure.

Producto/servicio de Verisure

Productos o sistemas desarrollados o fabricados por Verisure. Los productos, sistemas y datos que no sean propiedad de Verisure no están cubiertos por esta Política.

Preguntas y Asistencia

El equipo de seguridad de Verisure ha sido designado para gestionar la divulgación de Vulnerabilidades de seguridad. Puede ponerse en contacto con ellos rellenando y enviando el siguiente formulario.

Política de Divulgación Responsable del Grupo | Verisure