PROGRAMA DE DETECCION Y DIVULGACION DE VULNERABILIDADES DE LA COMUNIDAD

RPost es un líder mundial en comunicaciones electrónicas seguras y certificadas, basadas en sus tecnologías patentadas RMail®, RSign®, y Email Registrado™ para prueba de entrega, cifrado de correo electrónico, seguridad electrónica y tecnologías de firma electrónica. Millones de usuarios han disfrutado de servicios de RPost en más de 100 países, desde el año 2000.

RPost acepta informes de cualquier vulnerabilidad de nuestros servicios.

El Programa de Divulgación de Vulnerabilidad de RPost cubre inicialmente los siguientes productos:

- Servicio RMail® de Email Registrado™
- Servicio RMail® de Email Cifrado
- Servicios y Características de Firma Electrónica RMail®, RSign®, RForms™
- Servicios RMail® Gateway™
- Servicios RMail® y Características de Seguridad Electrónica y Uso Compartido de Archivos

Los investigadores que presenten un informe de vulnerabilidad recibirán todo el crédito en los boletines de seguridad publicados regularmente en RPost y en el sitio web de RPost si el informe merece un artículo.

Postura Legal

Las entidades corporativas y afiliadas de RPost no emprenderán acciones legales contra personas que presenten informes de vulnerabilidad para sus actividades en la identificación e información de la vulnerabilidad, tales actividades que consisten en:

- Participar en las pruebas de sistemas/investigación sin dañar a RPost o a sus clientes.
- Participar en pruebas de vulnerabilidad dentro del alcance de nuestro programa de divulgación de vulnerabilidades que no disminuyen la disponibilidad de servicios a los clientes.
- Pruebas en productos sin afectar a los clientes, o después de recibir el permiso/consentimiento de los clientes antes de participar en pruebas de vulnerabilidad contra sus dispositivos/ software, etc.
- Adherirse a las leyes de su ubicación y la ubicación de las entidades corporativas y afiliadas de RPost. Por ejemplo, violar leyes que sólo darían lugar a una reclamación de RPost (y no una reclamación penal) puede ser aceptable ya que RPost autoriza la actividad (ingeniería inversa o eludiendo medidas de protección) para mejorar su sistema.
- Abstenerse de revelar los detalles de vulnerabilidad al público antes de que expire un plazo mutuamente acordado.

Cómo reportar y enviar una vulnerabilidad

Los informes de vulnerabilidad deben presentarse a support@rpost.com. El correo electrónico del informe debe:

- Incluir "Informe de vulnerabilidad" o “Vulnerability Report” en la línea de asunto.
- Incluir información de contacto para la persona/organizaciones que envía el informe.
- Identificar el servicio RPost en el que se descubrió la vulnerabilidad.
- La hora y la fecha de las pruebas que revelaron la vulnerabilidad.
- Describa la naturaleza de la vulnerabilidad con suficiente detalle para permitir que el equipo de seguridad de RPost replique la vulnerabilidad.
- Si es posible, sugerencias para una posible remediación de la vulnerabilidad.

Criterios de Aceptación

RPost no aceptará un informe de vulnerabilidad a menos que contenga información suficiente para que el equipo de seguridad de RPost duplique la vulnerabilidad. Si la vulnerabilidad se desencadena por un formato o forma particular de mensaje o archivo adjunto, se debe incluir una copia del mensaje o los datos adjuntos relevantes. Si la vulnerabilidad se detectó mediante un servicio RPost protegido por contraseña, el informe debe incluir el nombre de usuario bajo el que se llevaron a cabo las pruebas.

Nuestro Compromiso

Los investigadores que informan de una vulnerabilidad pueden esperar:

- Una respuesta oportuna a su correo electrónico.
- Después del análisis, un informe sobre los pasos que RPost ha tomado o planea tomar para remediar la vulnerabilidad.
- Crédito público después de que la vulnerabilidad haya sido validada y corregida si el problema reportado merece un artículo.

Last Update: 15DIC20