5 de Mayo del 2017

Honorable Raúl Maldonado Gautier
Secretario de Hacienda

Honorable Carlos Contreras Aponte
Secretario de DTOP

Estimados secretarios:

Mi nombre es Anthony C. Rivera Carvelli, soy egresado de la Universidad de Puerto en Bayamón y actualmente trabajo como programador en Triple-S Vida. Escribo este mensaje para notificarles que sus páginas de internet sufren de una vulnerabilidad la cual permite que cualquier persona pueda ver el seguro social de un usuario de colecturía virtual con solo el nombre de usuario de esa persona. Cuando trato de acceder los servicios en línea de la página de DTOP me da un error el cual muestra exactamente donde está el error con lujo de detalle. Esto no debe de aparecer en una página cuando se encuentra en producción estos detalles son para los programadores cuando están desarrollando el programa ya que puede mostrar información sensitiva como próximamente veremos. En este error encuentro una dirección (hws.hacienda.gobierno.pr/cvservice/cvservices.asmx) la cual apunta al API de Hacienda. Una vez entro a esa página me presenta una lista de funciones que puedo ejecutar y una de ellas me permite ver el número de seguro social si poseo el nombre de usuario de colecturía virtual de esa persona.

Esto es un error craso y es un indicador de una mala configuración y programación. No existe ningún tipo de autenticación para las transacciones que efectué. Cualquier persona que entre a esa página o sepa la estructura de como enviar el SOAP request al servidor puede tener acceso a esa información. Como mínimo deben de validar quien puede hacer esas transacciones (SOAP request) para así limitar quien tiene acceso a esa información. Cualquier persona sin escrúpulos puede crear un programa para sacar los números de seguro social de su servicio. Me preocupa grandemente ver el patrón de mala programación y como la combinación de errores en ambas paginas lograron que este hueco de seguridad fuera posible. Del API de hacienda haber tenido una validación de quien hacía las transacciones no importa si pudiera ver la dirección no iba a poder ejecutar la función. Adjunto a este mensaje un archivo PDF con toda la información documentada de como pude conseguir los números de seguro social. Les dejo esto para que sus técnicos puedan replicar el problema para así poder solucionarlo. Cualquier cosa que necesiten no duden en contactarme.

Atentamente,

Anthony C. Rivera Carvelli