Vulnerabilidad De GoPro Expone Miles De contraseñas De Usuarios

GoPro, el fabricante de las populares cámaras de alta definición, tiene una **vulnerabilidad en la web oficial** que expone los nombres de usuario y contraseñas de miles de redes inalámbrica de sus clientes. Debido a los beneficios de estas cámaras, cada vez mas crece el numero de usuarios de este vestible para amantes de lo extremo.

GoPro ofrece una aplicación móvil para sus usuarios, lo que da un control remoto completo de todas las funciones de la cámara: tomar una foto, iniciar o detener la grabación y ajustar la configuración. Para lo anterior, es necesario conectar a la red inalámbrica que brinda la cámara, y la aplicación GoPro le da acceso instantáneo al Canal GoPro para ver fotografías y reproducir vídeos, y luego compartir sus archivos favoritos por correo electrónico, texto, Facebook, Twitter y más.

Falla Que Expone La Contraseña Inalámbrica

El investigador de seguridad **Ilya Chernyakov** informó que el proceso de ***actualización de GoPro*** podría exponer el nombre de usuario y la contraseña inalámbrica de los usuarios, lo cual podría ser de gran provecho para los atacantes informáticos.

Recientemente, **Chernyakov** pidió prestada una cámara GoPro a su amigo, quien olvidó la contraseña de su **cámara GoPro**. Así, que decidió recuperar la contraseña de la cámara mediante la **actualización del firmware de la cámara manualmente**, como se menciona en el sitio web GoPro.

> *Con el fin de obtener los archivos de actualización de la cámara, hay que seguir las instrucciones disponibles en el sitio web de GoPro. «Es un procedimiento bastante simple, con Siguiente -> Siguiente -.> Finalizar que termina con un enlace a un archivo zip. Al descargar este archivo, se obtiene un archivo zip que se supone que debes **copiar a la tarjeta SD**, ponerla en la GoPro y reiniciar la cámara «.*

El enlace del archvivo de descarga generada por el sitio web GoPro para el dispositivo de Chernyakov:

[bash]http://cbcdn2.gp-static.com/uploads/firmware-bundles/firmware_bundle/8605145/UPDATE.zip[/bash]

Cuando abrió el archivo archivo rar, se encontró un archivo llamado «***settings.in***«, el cual contenía las configuraciones deseadas de la cámara, incluyendo el nombre de la red inalámbrica y la contraseña en texto plano, como se muestra en la imagen:

¿Cómo Se Obtienen Miles De Contraseñas De GoPro?

Chernyakov notó que el sitio web GoPro no utiliza **ningún tipo de autenticación** para proporcionar el archivo de descarga para cada cliente, y tan solo con modificar el numero de la URL, se puede obtener el archivo personalizado de otros clientes.

Ademas, escribió un **script en Python** para descargar automáticamente el archivo para todos los números posibles de la misma serie y recaudó más de miles de nombres de usuario y contraseñas de redes inalámbricas, las cuales son usadas por los dueños de las cámaras GoPro.

Obviamente, la contraseña inalámbrica no sirven de nada a menos que el atacante no está en el rango de cualquier red inalámbrica específica, pero nombre de usuario, y contraseñas expuestas podría ser utilizadas por los atacantes para crear un diccionario para ataques de fuerza bruta.