Instagram, el servicio de Facebook para compartir fotos, corrigió recientemente una vulnerabilidad crítica que podría haber permitido a los piratas informáticos comprometer cualquier cuenta de Instagram sin requerir la interacción de los usuarios seleccionados.

La red social está creciendo rápidamente, y con la red de redes sociales más popular del mundo luego de Facebook, la red para compartir fotos domina absolutamente cuando se trata de la interacción y la interacción del usuario.

A pesar de contar con mecanismos de seguridad avanzados, las plataformas más grandes como Facebook, Google, LinkedIn e Instagram, no son completamente inmunes a los hackers y contienen muchas vulnerabilidades graves.

Algunas vulnerabilidades han sido parcheadas recientemente, algunos todavía están en proceso de ser reparadas, y muchas otras probablemente existen, pero no se han encontrado.

Los detalles de una de estas vulnerabilidades críticas en Instagram surgieron hoy en Internet que podrían haber permitido a un atacante remoto restablecer la contraseña de cualquier cuenta de Instagram y tomar el control completo sobre ella.

Descubierta y reportada de forma responsable por el cazador de recompensas de bugs indio, Laxman Muthiyah, la vulnerabilidad residía en el mecanismo de recuperación de contraseña implementado por la versión móvil de Instagram.

El restablecimiento de contraseña o recuperación de contraseña, es una función que permite a los usuarios recuperar el acceso a su cuenta en un sitio web, en caso de haber olvidado la contraseña.

En Instagram, los usuarios deben confirmar un código de acceso secreto de seis dígitos, que solo sirve durante los primeros 10 minutos, enviado a su número de teléfono o cuenta de correo asociado.

Esto significa que una de cada millón de combinaciones puede desbloquear cualquier cuenta de Instagram utilizando el ataque de fuerza bruta, pero no es tan simple como parece, ya que Instagram tiene habilitada la limitación de velocidad para prevenir dichos ataques.

Sin embargo, Laxman descubrió que esta limitación de velocidad se puede omitir enviando solicitudes de fuerza bruta desde diferentes direcciones IP y aprovechando la condición de carrera, enviando solicitudes simultáneas para procesar múltiples intentos de forma simultánea.

> *«El riesgo de carrera (solicitudes recurrentes) y la rotación de IP me permitieron evitarlo. De lo contrario, no sería posible. El tiempo de vencimiento de 10 minutos es la clave de su mecanismo de limitación de velocidad, por eso no impusieron el bloqueo permanente de códigos»,* dijo Laxman a THN.

Como se observa en el video, Laxman demostró con éxito la vulnerabilidad de secuestrar una cuenta de Instagram al intentar rápidamente 200 mil combinaciones diferentes de códigos de acceso sin ser bloqueado.

> *«En un escenario de ataque real, el atacante necesita 5000 IP para hackear una cuenta. Suena grande, pero en realidad es fácil si utiliza un proveedor de servicios en la nube como Amazon o Google. Costaría alrededor de 150 dólares realizar el ataque completo de un millón de códigos»,* dijo el investigador.

Laxman también lanzó un exploit de prueba de concepto para la vulnerabilidad, que ahora ha sido parcheado por Instagram, y la compañía otorgó a Laxman una recompensa de 30,000 dólares como parte de su programa de recompensas por errores.

Para evitar este tipo de ataques de fuerza bruta, se recomienda a los usuarios habilitar la función de «autenticación de dos factores».