Microsoft pagó a un investigador de seguridad independiente 50 mil dólares como parte de su programa de recompensas por errores, luego de que informó una falla que podría haber permitido a un actos malintencionado secuestrar las cuentas de los usuarios sin su conocimiento.

Informada por Laxman Muthiyah, la vulnerabilidad tiene como objetivo aplicar fuerza bruta al código de seguridad de siete dígitos que se envía a la dirección de correo electrónico o al número de teléfono móvil de un usuario para corroborar su identidad antes de restablecer la contraseña para recuperar el acceso a la cuenta.

Dicho de otra forma, el escenario de toma de control de la cuenta es una consecuencia de la escalada de privilegios que se deriva de una omisión de autenticación en un punto final que se utiliza para verificar los códigos enviados como parte del proceso de recuperación de la cuenta.

La compañía abordó el problema en noviembre de 2020, antes de que los detalles de la vulnerabilidad salieran a la luz este martes.

Aunque existen barreras de cifrado y controles de limitación de velocidad diseñados para evitar que un atacante envíe repetidamente los 10 millones de combinaciones de código de forma automática, Muthiyah dijo que finalmente descifró la función de cifrado utilizada para ocultar el código de seguridad y enviar múltiples solicitudes simultáneas.

Las pruebas de Muthiyah mostraron que de los 1000 códigos que se enviaron, solo 122 pasaron, y los demás se bloquearon con el código de error 1211.

> *«Me di cuenta de que se agregan a listas negras de direcciones IP si todas las peticiones que enviamos no golpean el servidor al mismo tiempo. Unos pocos milisegundos de retardo entre las solicitudes permitió al servidor detectar el ataque y bloquearlo»,* dijo el investigador.

Después del descubrimiento, Muthiyah dijo que pudo sortear la restricción de limitación de velocidad y llegar al siguiente paso de cambiar la contraseña, lo que le permitió secuestrar la cuenta.

Aunque el ataque solo funciona en los casos en que la cuenta no está protegida por la autenticación de dos factores, aún se puede extender para anular las dos capas de protección y modificar la contraseña de una cuenta objetivo, lo que podría ser prohibitivo debido a la cantidad de recursos informáticos necesarios para montar un ataque de este tipo.

> *«Poniendo todo junto, un atacante tiene que enviar todas las posibilidades de códigos de seguridad de 6 y 7 dígitos que serían alrededor de 11 millones de intentos de solicitud, y tiene que enviarse al mismo tiempo para cambiar la contraseña de cualquier cuenta de Microsoft (Incluso aquellas con 2FA habilitado)»,* dijo Muthiyah.

De forma separada, Muthiyah también empleó una técnica similar al flujo de recuperación de la cuenta de Instagram, al enviar 200 mil solicitudes simultáneas desde 1000 máquinas diferentes, descubriendo que era posible lograr el secuestro de la cuenta. Por esto, fue recompensado con 30,000 dólares como parte del programa de recompensas de la compañía.

> *«En un escenario de ataque real, el atacante necesita 5000 direcciones IP para hackear una cuenta. Parece 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.