Twitter reveló el viernes que se utilizó una vulnerabilidad de día cero ya parcheada para vincular números de teléfono y correos electrónicos a cuentas de usuarios en la plataforma de redes sociales.

> *«Como resultado de la vulnerabilidad, si alguien envió una dirección de correo electrónico o un número de teléfono a los sistemas de Twitter, los sistemas de Twitter le dirían a la persona a qué cuenta de Twitter se asoció la dirección de correo electrónico o el número de teléfono enviado, si corresponde»,* dijo la compañía en un comunicado.

Twitter dijo que el error, del que se informó en enero de 2022, se debió a un cambio de código introducido en junio de 2021. No se expusieron contraseñas como resultado del incidente.

El retraso de seis meses en hacer el anuncio público se deriva de la nueva evidencia del mes pasado sobre un actor no identificado que se había aprovechado potencialmente de la vulnerabilidad antes de la corrección para extraer información del usuario y venderla con fines de lucro en Breach Forums.

Aunque Twitter no reveló el número exacto de usuarios afectados, la publicación en el foro realizada por el atacante muestra que la falla fue explotada para compilar una lista que supuestamente contiene más de 5.48 millones de perfiles de cuentas de usuarios.

Restore Privacy, que reveló la violación a fines del mes pasado, dijo que la base de datos se vendía por 30,000 dólares.

Twitter declaró que está en proceso de notificar directamente a los propietarios de cuentas afectados por el problema, al mismo tiempo que insta a los usuarios a activar la autenticación de dos factores para protegerse contra inicios de sesión no autorizados.

El desarrollo se produce cuando Twitter, en mayo, acordó pagar una multa de 150 millones

de dólares para resolver una queja del Departamento de Justicia de Estados Unidos, que alegaba que la compañía entre 2014 y 2019 usó información proporcionada por los titulares de cuentas para verificación de seguridad con fines publicitarios sin su consentimiento.