Investigadores de seguridad cibernética revelaron detalles de vulnerabilidades ya reparadas en Zendesk Explore, que podrían haber sido aprovechadas por un atacante para obtener acceso no autorizado a la información de las cuentas de los clientes que tienen la función activada.

> *«Antes de que se reparara, la vulnerabilidad había permitido a los atacantes acceder a conversaciones, direcciones de correo electrónico, tickets, comentarios y otra información de las cuentas de Zendesk con Explore habilitado»*, dijo Varonis en un informe.

La compañía de seguridad cibernética dijo que no había evidencia que sugiriera que los problemas se explotaron activamente en ataques del mundo real. No se requiere ninguna acción por parte de los clientes.

Zendesk Explore es una solución de informes y análisis que permite a las organizaciones *«ver y analizar información clave sobre sus clientes y sus recursos de soporte».*

Según la compañía de software de seguridad, la explotación de la deficiencia primero requiere que un atacante se registre en el servicio de tickets de la cuenta de Zendesk de su víctima como un nuevo usuarios externo, una función que probablemente esté habilitada de forma predeterminada para permitir que los usuarios finales envíen tickets de soporte.

La vulnerabilidad se relaciona con una inyección SQL en su API GraphQL que podría abusarse para filtrar toda la información almacenada en la base de datos como usuario administrador, incluidas direcciones de correo electrónico, tickets y conversaciones con agentes en vivo.

Una segunda vulnerabilidad se refiere a un problema de acceso a la lógica asociado con una API de ejecución de consultas, que se configuró para ejecutar las consultas sin verificar si el *«usuario»* que realiza la llamada tenía el permiso adecuado para hacerlo.

> *«Esto significaba que un usuario final recién creado podía invocar esta API, cambiar la consulta y robar datos de cualquier tabla en el RDS de la cuenta de Zendesk de destino, sin necesidad de SQLi».*

Varonis dijo que los problemas fueron revelados a Zendesk el 30 de agosto, después de lo cual la empresa corrigió las fallas el 8 de septiembre de 2022.