Investigadores en ciberseguridad están alertando sobre el hallazgo de miles de sitios de comercio electrónico Oracle NetSuite con acceso externo, que se han encontrado vulnerables a la filtración de información sensible de los clientes.

> *«Un posible problema en la plataforma SuiteCommerce de NetSuite podría permitir que atacantes accedan a datos sensibles debido a configuraciones incorrectas de los controles de acceso en tipos de registros personalizados (CRTs, por sus siglas en inglés),»* mencionó Aaron Costello de AppOmni.

Es importante subrayar que este problema no se debe a una debilidad en la seguridad del producto NetSuite, sino a una configuración incorrecta por parte del cliente, lo que puede provocar la exposición de datos confidenciales. La información filtrada incluye direcciones completas y números de teléfono móvil de los clientes registrados en estos sitios de comercio electrónico.

El escenario de ataque descrito por AppOmni aprovecha CRTs que utilizan controles de acceso a nivel de tabla con el tipo de acceso *«No se requiere permiso»*, lo que permite a usuarios no autenticados acceder a la información utilizando las API de registros y búsqueda de NetSuite.

Sin embargo, para que este ataque tenga éxito, hay ciertos requisitos previos, siendo el principal que el atacante debe conocer los nombres de los CRTs en uso.

Para reducir el riesgo, se recomienda que los administradores de los sitios refuercen los controles de acceso en los CRTs, configuren los campos sensibles en «Ninguno» para el acceso público, y consideren desconectar temporalmente los sitios afectados para evitar la exposición de datos.

> *«La solución más sencilla desde una perspectiva de seguridad podría ser cambiar el Tipo de Acceso de la definición del tipo de registro a 'Requerir Permiso para*

> *Entradas de Registros Personalizados' o 'Usar Lista de Permisos',»* comentó Costello.

Esta revelación coincide con el detalle proporcionado por Cymulate sobre una forma de manipular el proceso de validación de credenciales en Microsoft Entra ID (anteriormente conocido como Azure Active Directory) y eludir la autenticación en infraestructuras de identidad híbrida, lo que permite a los atacantes iniciar sesión con altos privilegios dentro del tenant y establecer persistencia.

No obstante, para llevar a cabo este ataque, un adversario necesita tener acceso administrativo en un servidor que aloje un agente de Autenticación de Paso a Través (PTA, por sus siglas en inglés), un módulo que permite a los usuarios iniciar sesión en aplicaciones tanto locales como basadas en la nube utilizando Entra ID. El problema surge en Entra ID cuando se sincronizan varios dominios locales con un solo tenant de Azure.

> *«Este problema se presenta cuando las solicitudes de autenticación son mal gestionadas por los agentes de autenticación de paso a través (PTA) para diferentes dominios locales, lo que podría resultar en acceso no autorizado,»* señalaron los investigadores de seguridad Ilan Kalendarov y Elad Beber.
>
> *«Esta vulnerabilidad convierte al agente PTA en un agente doble, permitiendo a los atacantes iniciar sesión como cualquier usuario sincronizado de AD sin conocer su contraseña real; esto podría potencialmente dar acceso a un usuario con privilegios de administrador global si se le han asignado.»*