Los expertos en seguridad informática han descubierto un caso de aumento de privilegios relacionado con una aplicación de Microsoft Entra ID (anteriormente Azure Active Directory) al aprovechar una URL de respuesta no utilizada.

> *«Un atacante podría aprovechar esta URL desatendida para redirigir códigos de autorización hacia sí mismo, intercambiando los códigos obtenidos de forma ilegal por tokens de acceso»,* mencionó el informe técnico publicado la semana pasada por la Unidad de Contramedidas de Amenazas Seguras (CTU) de Secureworks.

> *«Luego, el actor malicioso podría utilizar un servicio intermedio para llamar a la API de Power Platform y obtener privilegios elevados».*

Después de una divulgación responsable el 5 de abril de 2023, Microsoft solucionó el problema mediante una actualización lanzada un día después. Secureworks también ha proporcionado una herramienta de código abierto que otras organizaciones pueden utilizar para buscar URLs de respuesta no utilizadas.

La URL de respuesta, también conocida como URI de redirección, hace referencia al lugar al que el servidor de autorización dirige al usuario una vez que la aplicación ha sido autorizada con éxito y se le ha concedido un código de autorización o un token de acceso.

> *«Es importante registrar la ubicación correcta como parte del proceso de registro de la aplicación, ya que el servidor de autorización enviará el código o token a la URI de redirección»,* señala la documentación de Microsoft.

El equipo CTU de Secureworks descubrió una URL de respuesta abandonada asociada a la aplicación Dynamics Data Integration y al perfil del Azure Traffic Manager. Esto permitía invocar la API de Power Platform a través de un servicio intermedio y manipular las

configuraciones del entorno.

En un escenario hipotético de ataque, esto podría haberse utilizado para obtener el rol de administrador del sistema para un principal de servicio existente y enviar solicitudes para eliminar un entorno, así como abusar de la API del Azure AD Graph para recopilar información sobre el objetivo y llevar a cabo actividades posteriores.

Sin embargo, esto depende de que una víctima haga clic en un enlace malicioso, lo cual permitiría al actor amenazante redirigir el código de autorización emitido por Microsoft Entra ID hacia una URL de redirección secuestrada.

Esta revelación se produce mientras Kroll reveló un aumento en las campañas de phishing con temática de DocuSign que utilizan redirecciones abiertas. Esto permite a los adversarios propagar URLs especialmente diseñadas que, al hacer clic en ellas, redirigen a las posibles víctimas hacia un sitio malicioso.

> *«Al crear una URL engañosa que utiliza un sitio web confiable, los actores maliciosos pueden manipular más fácilmente a los usuarios para que hagan clic en el enlace y evadir la tecnología de red que escanea los enlaces en busca de contenido malicioso»,* dijo George Glass de Kroll.

> *«Esto resulta en que la víctima sea redirigida hacia un sitio malicioso diseñado para robar información confidencial, como credenciales de inicio de sesión, detalles de tarjetas de crédito o datos personales».*