Investigadores en ciberseguridad han identificado dos fallas de seguridad en el servicio Azure Health Bot de Microsoft que, si se explotan, podrían permitir a un atacante malicioso moverse lateralmente dentro de los entornos de los clientes y acceder a información confidencial de pacientes.

Microsoft ya ha solucionado estos problemas críticos, que podrían haber permitido el acceso a recursos compartidos entre distintos inquilinos dentro del servicio, según un nuevo informe de Tenable.

El servicio Azure AI Health Bot es una plataforma en la nube que facilita a los desarrolladores de organizaciones de salud la creación y despliegue de asistentes virtuales de salud impulsados por inteligencia artificial, y la generación de copilotos para manejar tareas administrativas y comunicarse con los pacientes.

Esto incluye bots desarrollados por proveedores de seguros para que los clientes puedan verificar el estado de sus reclamaciones y realizar consultas sobre beneficios y servicios, así como bots utilizados por entidades de atención médica para ayudar a los pacientes a encontrar la atención adecuada o localizar médicos cercanos.

La investigación de Tenable se centró en un componente específico del servicio Azure AI Health Bot denominado Data Connections, que, como sugiere su nombre, permite la integración de datos de fuentes externas, ya sean de terceros o de las API propias de los proveedores de servicios.

Aunque esta función cuenta con medidas de seguridad integradas para evitar el acceso no autorizado a las API internas, una investigación adicional reveló que estas protecciones podían ser sorteadas mediante la emisión de respuestas de redirección (códigos de estado 301 o 302) al configurar una conexión de datos utilizando un servidor externo bajo control del atacante.

Configurando el servidor para responder a solicitudes con una respuesta de redirección 301 dirigida al servicio de metadatos de Azure (IMDS), Tenable señaló que se podía obtener una

respuesta válida de metadatos y luego adquirir un token de acceso para management.azure[.]com.

El token podría emplearse para enumerar las suscripciones a las que brinda acceso mediante una llamada a un punto de conexión de Microsoft, que a su vez devuelve una ID de suscripción interna, la cual podría aprovecharse para listar los recursos accesibles al llamar a otra API.

Además, se descubrió que otro punto de conexión relacionado con la integración de sistemas que soportan el formato de intercambio de datos Fast Healthcare Interoperability Resources (FHIR) era igualmente vulnerable al mismo tipo de ataque.

Tenable informó a Microsoft sobre estos hallazgos en junio y julio de 2024, después de lo cual la compañía comenzó a implementar soluciones en todas las regiones. No hay indicios de que la vulnerabilidad haya sido explotada activamente.

> *«Las fallas de seguridad suscitan preocupaciones sobre cómo los chatbots podrían ser explotados para exponer información confidencial. En particular, las vulnerabilidades estaban relacionadas con un defecto en la arquitectura subyacente del servicio de chatbot, subrayando la relevancia de la seguridad tradicional de aplicaciones web y en la nube en la era de los chatbots impulsados por IA»,* señaló Tenable en un comunicado.

La revelación se produce pocos días después de que Semperis describiera una técnica de ataque llamada UnOAuthorized, que permite la escalada de privilegios a través de Microsoft Entra ID (anteriormente conocido como Azure Active Directory), lo que incluye la posibilidad de agregar y eliminar usuarios de roles con privilegios. Microsoft ya ha corregido la brecha de seguridad.

> *«Un actor malintencionado podría haber utilizado dicho acceso para obtener*

> *privilegios de Administrador Global e implementar métodos adicionales de persistencia en un inquilino. Un atacante también podría usar este acceso para realizar movimientos laterales en cualquier sistema de Microsoft 365 o Azure, así como en cualquier aplicación SaaS conectada a Entra ID»,* explicó el investigador de seguridad Eric Woodruff.