Se han revelado detalles sobre tres vulnerabilidades de seguridad, ya corregidas, en Dynamics 365 y Power Apps Web API que podrían haber causado la exposición de información confidencial.

Estas vulnerabilidades, identificadas por la empresa australiana de ciberseguridad Stratus Security, fueron solucionadas en mayo de 2024. Dos de los problemas estaban relacionados con el filtro de la API OData Web de Power Platform, mientras que la tercera vulnerabilidad estaba vinculada a la API FetchXML.

El primer problema de seguridad se originaba en la ausencia de controles de acceso adecuados en el filtro de la API OData Web, lo que permitía acceder a la tabla de contactos. Esta tabla contenía datos sensibles, como nombres completos, números de teléfono, direcciones, información financiera y hashes de contraseñas.

Un atacante podría aprovechar esta falla para realizar búsquedas booleanas y descifrar el hash completo, probando cada carácter del hash de forma secuencial hasta encontrar el valor correcto.

> *«Por ejemplo, comenzamos enviando* `startswith(adx_identity_passwordhash, 'a')`*, luego* `startswith(adx_identity_passwordhash, 'aa')`*, después* `startswith(adx_identity_passwordhash, 'ab')`*, y así sucesivamente hasta obtener resultados que comiencen con 'ab'»,* explicó Stratus Security.
>
> *«Seguimos este procedimiento hasta que la consulta no devuelva más resultados válidos con caracteres adicionales, lo que nos indica que hemos recuperado el valor completo.»*

La segunda vulnerabilidad estaba relacionada con el uso de la cláusula `orderby` en la misma API, que permitía extraer información de columnas específicas de la base de datos, como `EMailAddress1`, que corresponde a la dirección de correo electrónico principal del contacto.

Por último, Stratus Security identificó que la API FetchXML también podía explotarse junto con la tabla de contactos para acceder a columnas restringidas mediante consultas con la cláusula `orderby`.

> *«Al emplear la API de FetchXML, un atacante puede crear una consulta 'orderby' sobre cualquier columna, pasando por alto por completo los mecanismos de control de acceso existentes. A diferencia de vulnerabilidades previas, este enfoque no necesita que el 'orderby' esté en orden descendente, lo que proporciona mayor flexibilidad al ataque»*, explicó.

Un atacante que explote estas vulnerabilidades podría, en consecuencia, generar un listado de hashes de contraseñas y correos electrónicos, para después descifrar dichas contraseñas

o comercializar los datos obtenidos.

> *«El hallazgo de fallas en la API de Dynamics 365 y Power Apps resalta un punto clave: la seguridad cibernética exige una atención constante, especialmente para corporaciones como Microsoft, que gestionan grandes volúmenes de información»*, destacó Stratus Security.