



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.»



```
Request
Pretty Raw Hex
1 GET /_api/contacts?select=emailaddress1 HTTP/1.1
2 Host: stratus-poc-1.powerappsportals.com
3 Cookie: Dynamics365PortalAnalytics=
W4cJ7-R1cqM_3tQ2GvOmc979m9H0mwqt1g9kq3xcmEDPmx1eMtyWAAM1WzSP
OWyMdeESS6Us_BvYoNoVKsV-FnVksV_212VYQjvfpdO6Pz-65_oapKXcZmpA
BJqJTYvIqDRÄe5F43fP5hg94s4knwÄ2; ARRAffinity=
Bccifa015b5ad9831446c4dda081bde58ff122211e0c831aadd5d8af3533
0d02; ARRAffinitySameSite=
Bccifa015b5ad9831446c4dda081bde58ff122211e0c831aadd5d8af3533
0d02
4 Sec-Ch-Ua: "Chromium";v="121", "Not A|Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85
Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Priority: u=0, i
17 Connection: close

Response
Pretty Raw Hex Render
1 HTTP/1.1 403 Forbidden
2 Content-Length: 262
3 Connection: close
4 Content-Type: application/json; charset=utf-8
5 Date: Tue, 06 Feb 2024 03:28:15 GMT
6 Cache-Control: no-cache
7 Expires: -1
8 Pragma: no-cache
9 Strict-Transport-Security: max-age=31536000; includeSubDomains;
preload
10 x-ms-request-id: 102c3616-803f-49cb-8b05-791f9bbb4c30
11 x-ms-portal-app: site-a0001a95-b8es-4fa9-a25c-aaf7elfac8d7-AUe
12 X-Frame-Options: SAMEORIGIN
13
14 {
  "error": {
    "code": "90040101",
    "message":
      "Attribute emailaddress1 in table contact is not enabled fo
r Web Api.",
    "innererror": {
      "code": "90040101",
      "message":
        "Attribute emailaddress1 in table contact is not enabled
for Web Api.",
      "type": "AttributePermissionIsMissing"
    }
  }
}
```

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.