# Broken Access Control on U.S. Dept. of State Visa Scheduling System Leading to Mass PII Exposure

**Vulnerability:** Broken Access Control / Insecure Direct Object Reference (IDOR)

**Target:** `acs.usvisascheduling.com` (U.S. Department of State)

**Severity:** Critical / High (CVSS 8.1)

**Status:** Patched / Resolved

---

## Executive Summary

During a security assessment of the U.S. Department of State's visa scheduling portal ( `usvisascheduling.com` ), I discovered a critical Broken Access Control vulnerability in the Microsoft Dynamics 365 Web API implementation. The application failed to enforce Object-Level Authorization on the `/_api/contacts` endpoint.

This vulnerability allowed any authenticated user (regardless of privilege level) to query the global contacts database. The response returned sensitive Personally Identifiable Information (PII) for thousands of other visa applicants, including full names, email addresses, internal GUIDs, and most critically, plaintext password reset tokens/temporary passwords.

---

## Technical Analysis

The application utilizes Microsoft Dynamics 365 for its backend customer relationship management (CRM). The frontend application interacts with this backend via the OData Web API.

### The Flaw

The vulnerability existed because the default OData endpoint `/_api/contacts` was exposed to the public internet without proper scoping or access controls. While the application required authentication to reach the endpoint, it did not check if the requesting user *owned* the data they were requesting.

By default, the Dynamics 365 Web API should be configured to restrict read access to the user's own record (e.g., `/_api/contacts(current-user-guid)` ). However, the configuration allowed a "global read" operation on the `contacts` entity set.

### Exposed Data Fields

The JSON response leaked extensive internal and external user data. Key fields observed included:

- `fullname` : The applicant's full legal name.
- `emailaddress1` : Personal email addresses (e.g., `@gmail.com` ).
- `adx_identity_username` : The username used for login.
- `adx_identity_newpassword` : **Critical.** This field appeared to contain plaintext temporary passwords or reset tokens.
- `contactid` : Internal unique GUIDs for users.
- `atlas_userstage` : The current status of the user's visa application (e.g., "Application Closed", "Registration Complete").

---

## Proof of Concept (Reproduction)

The exploitation path was trivial and required low technical skill, increasing the risk factor.

1. **Authentication:** I logged into a valid, low-privileged applicant account on `https://acs.usvisascheduling.com` .
2. **Endpoint Manipulation:** I manually modified the browser URL from the user dashboard to the API endpoint:

```
GET https://acs.usvisascheduling.com/_api/contacts
```

3. **Data Extraction:** The server responded with a `200 OK` status and a JSON payload containing the user database.
4. **Verification:** I verified the presence of other users' PII in the response body, confirming that the scope was not limited to my own account.

**Code Snippet (Reconstructed JSON Response):**

```
{
  "value": [
    {
      "fullname": "Jane Doe",
      "emailaddress1": "jane.doe@example.com",
      "adx_identity_newpassword": "TemporaryPassword123!",
      "adx_identity_username": "janedoe2025",
      "contactid": "a1b2c3d4-e5f6-7890-...."
    },
  ]
}
```

## Impact Assessment

The impact of this vulnerability was classified as **High** due to the sensitivity of the data and the ease of exploitation.

- **Account Takeover (ATO):** The exposure of the `adx_identity_newpassword` field (likely used for account setups or resets) combined with usernames and emails provided a direct path for attackers to fully compromise victim accounts.
- **Mass PII Harvesting:** An attacker could write a simple script to iterate through the API pagination and dump the entire database of visa applicants.
- **Targeted Phishing/Social Engineering:** With knowledge of a user's full name, email, and exact "Application Status" (e.g., "Registration Complete"), an attacker could craft highly convincing phishing emails pretending to be consular staff.
- **National Security/Privacy Risk:** The exposure of foreign nationals' data and their visa application statuses poses a significant privacy violation and potential diplomatic risk.

## Remediation & Fix

To resolve this issue, I recommended the following remediation steps to the Department of State engineering team:

1. **Implement Object-Level Authorization:** Ensure that the API validates the requesting `user_id` against the requested resource. Users should only be able to query their own `contactid`.
2. **Restrict API Permissions:** Configure the Dynamics 365 Web API to deny access to the global `contacts` entity set for the "Authenticated Users" role.
3. **Field-Level Security:** Specifically explicitly exclude sensitive columns like `adx_identity_newpassword` and `adx_identity_securitystamp` from API responses entirely, regardless of user privileges.

## Timeline

- **December 22, 2025:** Vulnerability discovered and reported to U.S. Dept of State VDP via HackerOne.
- **December 23, 2025:** Triage team requested clarification on sensitive information and impact.
- **December 28, 2025:** I provided a detailed impact analysis demonstrating the password leak and PII exposure.
- **December 30, 2025:** Report Validated and Triaged.
- **January 8, 2026:** Internal severity assessed as **High (8.1)**. Issue forwarded for remediation.
- **January 15, 2026:** Vulnerability remediated, and was retested by me.

> **Researcher:** Abdiel Y. Vega Velez
> **Email:** abdiel.vega@outlook.com
> **HackerOne Username:** notaquacc