Authorization Bypass in Federal Visa Portal Leading to Mass PII Exposure

Vulnerability Class: Broken Access Control / IDOR

Severity: High (CVSS ~8.1)

Status: Retesting (Open)

Date Triaged: December 10, 2025

Executive Summary

During a authorized security assessment for the U.S. Department of State Vulnerability Disclosure Program (VDP), I identified a critical **Broken Access Control** vulnerability within a public-facing visa scheduling system.

The application's API failed to enforce Object-Level Authorization, allowing any authenticated user to access the personal records of other applicants. This flaw exposed sensitive Personally Identifiable Information (PII) including full legal names, email addresses, and account recovery tokens, creating a direct vector for mass account takeovers and targeted phishing campaigns against foreign nationals.

Technical Analysis

The application leverages a Customer Relationship Management (CRM) backend to handle applicant data. The frontend communicates with this backend via a RESTful API.

The Vulnerability: Insecure Direct Object Reference (IDOR)

The vulnerability stems from an insecure implementation of the OData API protocol. While the application correctly enforces authentication (requiring a user to be logged in), it fails to validate **data ownership** for API requests.

In a secure environment, when a user requests their profile data, the server should verify that the `user_id` in the request matches the session of the requester. In this instance, the API endpoint responsible for retrieving contact details was configured with "Global Read" permissions for authenticated users.

This allowed a threat actor to manipulate the API query to request the records of *other* users rather than their own, bypassing the intended application logic.

Sensitive Data Exposure

The API response returned a raw JSON object containing extensive user data. The most critical exposed fields included:

- **Identity Data:** Full Legal Name and Internal User GUIDs.
- **Contact Information:** Personal email addresses.
- **Account Secrets:** Plaintext temporary passwords and password reset tokens (allowing for immediate account takeover).
- **Visa Status:** Granular details on the user's application stage (e.g., "Registration Complete," "Application Closed").

Impact Assessment

Due to the ease of exploitation and the sensitivity of the data, this vulnerability was classified as **Critical/High**.

- **Account Takeover (ATO):** The exposure of password reset tokens allows an attacker to reset passwords for arbitrary users and seize control of their accounts.
- **Mass PII Harvesting:** An attacker could script the enumeration of the database, potentially scraping thousands of records per hour.
- **State-Sponsored Threats:** The exposure of visa application statuses and foreign national data poses a significant geopolitical and privacy risk, potentially aiding state-level surveillance or social engineering.

Recommendation & Remediation

I provided the following remediation strategy to the agency's team:

1. **Enforce Object-Level Security:** Implement server-side checks to validate that the requesting user's `Subject ID` matches the `Resource ID` being accessed.

2. **Restrict "Global Read" Permissions:** Modify the CRM security roles to ensure the "Authenticated Users" group does not have read access to the global contact entity set.
3. **Field-Level Redaction:** Specifically exclude high-risk columns (such as password tokens) from API responses entirely, regardless of user privilege.

Disclosure Timeline

- **December 2025:** Vulnerability identified and reported via official VDP channels.
- **December 2025:** Report triaged; impact demonstrated via sanitized Proof of Concept.
- **January 2026:** Severity assessed as **High**; issue currently in remediation queue.

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