INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-27 18:54 UTC

Uruguayan Government Data Breach: 5.8 Million Citizen Records Exposed in Latin American Government Targeting Campaign

DATA BREACH | HIGH | CVSS 5.0

SCC Item ID	SCC-DBR-2026-0141
Type	Data Breach
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Uruguayan government agencies (unspecified); citizen PII records
Published	2026-05-27T12:19:03
Discovery Source	Rss

Executive Summary

An unattributed threat actor has claimed to have leaked approximately 5.8 million Uruguayan citizen records - roughly 1.7 times Uruguay's population of 3.4 million - indicating aggregation across multiple government databases or historical sources. The breach claim follows a documented pattern of Latin American cybercriminal operations targeting government agencies to exfiltrate and sell citizen PII at scale. For organizations with Uruguayan operations, vendor relationships, or employees with Uruguayan identity documentation, the risk of downstream fraud, social engineering, and identity compromise is elevated.

Technical Analysis

Threat actor claims to have exfiltrated approximately 5.8 million citizen PII records from unspecified Uruguayan government agencies. The record count exceeding Uruguay's 3.4 million population suggests cross-database aggregation, inclusion of diaspora records, or historical data accumulation, a pattern consistent with prior Latin American government breach claims. No CVE is associated. Probable attack vectors include exploitation of externally exposed government APIs or databases with insufficient access controls (CWE-284: Improper Access Control), resulting in alleged unauthorized data disclosure (CWE-200: Exposure of Sensitive Information to an Unauthorized Actor; CWE-359: Exposure of Private Personal Information to an Unauthorized Actor). MITRE ATT&CK techniques mapped: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1213 (Data from Information Repositories), T1530 (Data from Cloud Storage), T1041 (Exfiltration Over C2 Channel), T1567 (Exfiltration Over Web Service), T1657 (Financial Theft), T1589.002 (Gather Victim Identity Information: Email Addresses). Attribution is unconfirmed. Affected data types are unverified; identity, demographic, and contact

data are suspected based on regional incident patterns. No patch status is applicable; remediation is access control and data governance focused. Discovery source is RSS feed aggregation; claims require validation against official Uruguayan government or CERTuy disclosures before treating as confirmed.

Action Checklist

1. Step 1: Exposure Assessment. Determine whether your organization holds data dependencies on Uruguayan government identity systems or processes Uruguayan citizen PII. Audit third-party integrations, onboarding workflows, or vendor relationships that rely on government-sourced identity verification from Uruguay. Reference CIS 3.2 (Establish and Maintain a Data Inventory) to locate where Uruguayan citizen data is stored or transited in your environment.
2. Step 2: Detection. Monitor threat intelligence feeds, dark web monitoring platforms, and paste sites for samples of the claimed dataset. Search for Uruguayan national ID patterns (Cédula de Identidad format) or government domain indicators in your inbound data flows. Review logs for anomalous API query volumes against any government-facing integrations. Apply NIST SP 800-53 AU-6 (Audit Record Review, Analysis, and Reporting) to examine access logs for data repositories holding Uruguayan citizen records. Behavioral indicator: bulk data export or query activity against citizen identity databases at unusual hours.
3. Step 3: Eradication. If your organization hosts or mirrors Uruguayan government data, audit access control configurations immediately against NIST SP 800-53 AC-3 (Access Enforcement) and AC-6 (Least Privilege). Revoke unnecessary API keys, service accounts, or external access grants touching citizen PII repositories. Rotate credentials for any accounts with read access to affected data stores per NIST SP 800-53 IA-4 (Identifier Management). Apply NIST SP 800-53 AC-2 (Account Management) to restrict data repository access to verified, role-justified accounts only.
4. Step 4: Recovery. Validate that access control changes are enforced and logged. Confirm MFA is active on all accounts with access to citizen PII repositories (NIST SP 800-53 IA-2; CIS 6.3, CIS 6.5). Review NIST SP 800-53 AU-9 (Protection of Audit Information) to ensure audit logs covering affected repositories are intact, tamper-evident, and retained per AU-11. Monitor for follow-on social engineering targeting employees with Uruguayan-origin credentials or contacts; this data class frequently fuels spear-phishing campaigns.
5. Step 5: Post-Incident. Conduct a control gap review focused on CWE-284 and CWE-200: audit all externally exposed APIs and database interfaces for missing authentication, authorization enforcement, and rate limiting. Evaluate whether your organization's data minimization practices align with CIS 3.3 (Configure Data Access Control Lists) and CIS 3.4 (Enforce Data Retention). Brief third-party vendors processing Uruguayan citizen data on the breach claim and request their exposure assessments. Document findings for regulatory reporting purposes where applicable under data protection obligations.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to legal, privacy counsel, and executive leadership if internal data inventory confirms your organization stores or has processed Uruguayan citizen Cédula de Identidad numbers, names, or addresses — at that point, breach notification obligations under applicable data protection frameworks (e.g., Uruguay's Law 18.331, GDPR for EU-linked operations, or sector-specific regulations) may be triggered and legal hold requirements activate.
Recovery Notes	Post-containment, maintain heightened monitoring of all authentication events and inbound email for a minimum of 90 days, given that 5.8 million records of Uruguayan citizen PII — including national ID numbers — provide threat actors with persistent, high-quality material for targeted spear-phishing and credential stuffing campaigns against your employees or customers with Uruguayan identity ties. Verify that all API endpoints previously integrated with Uruguayan government identity verification services are either disabled, rate-limited, and authenticated, or formally decommissioned with integration dependencies removed. Confirm with third-party vendors that they have completed their own exposure assessments and document their responses, as downstream liability exposure depends on the thoroughness of your vendor notification and follow-up chain.
Forensic Artifacts	Database query audit logs (PostgreSQL pg_audit extension output or MySQL general_log) capturing SELECT operations returning Uruguayan citizen record fields — specifically bulk or unbounded queries against tables containing Cédula de Identidad, nombre completo, fecha de nacimiento, or domicilio columns, timestamped against the breach claim disclosure date | API gateway access logs (AWS API Gateway CloudWatch logs, NGINX access.log, or equivalent) for *.gub.uy-referencing endpoints showing request volume anomalies, large response payload sizes, or sequential Cédula number enumeration patterns indicative of automated scraping | Outbound network flow records (NetFlow, firewall session logs) filtered for large data transfers (>10MB sessions) to non-baseline external IPs or known data broker infrastructure, occurring in the weeks preceding the public breach claim — this is the likely exfiltration window | Authentication logs (Windows Security Event ID 4624/4625 or Linux /var/log/auth.log) for service accounts with citizen PII database access, reviewed for logon events from unexpected source IPs, geographic anomalies, or off-hours activity patterns consistent with threat actor lateral movement or data staging | Dark web and paste site monitoring artifacts: saved copies of any claimed dataset samples circulating on criminal forums (BreachForums, Telegram channels targeting LATAM government data) containing Cédula de Identidad number ranges, used to cross-reference against your organization's known data holdings and confirm whether your data subset was included in the aggregated leak

Per-Action IR Details

Step 1: Exposure Assessment — Determine whether your organization holds data dependencies on Uruguayan government identity systems or processes Uruguayan citizen PII. Audit third-party integrations, onboarding workflows, or vendor relationships that rely on government-sourced identity verification from Uruguay. Reference CIS 3.2 (Establish and Maintain a Data Inventory) to locate where Uruguayan citizen data is stored or transited in your environment.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish IR capability and identify data assets at risk prior to or at breach notification

Controls: CIS 3.2 (Establish and Maintain a Data Inventory), NIST RA-2 (Security Categorization), NIST PM-5 (System Inventory), NIST AC-20 (Use of External Systems)

Compensating: Run a grep or PowerShell search across file shares and database exports for Uruguayan Cédula de Identidad number patterns (7-8 digit numeric strings associated with .uy domains or 'Uruguay' metadata fields):

PowerShell — `Get-ChildItem -Recurse | Select-String -Pattern '\b[1-9]\d{6,7}\b'` against data directories. Use osquery (`SELECT * FROM file WHERE path LIKE '/data/%' AND filename LIKE '*uruguay*';`) to enumerate relevant files. Map vendor API endpoints by reviewing outbound network connections in Wireshark or firewall exports filtered to Uruguayan government IP ranges (e.g., *.gub.uy domains).

Evidence: Before executing data inventory queries, preserve: (1) current third-party API integration configuration files and connection strings referencing Uruguayan identity providers or *.gub.uy endpoints; (2) vendor contract or data processing agreement documents specifying Uruguayan citizen PII handling; (3) existing data flow diagrams or network topology records showing ingestion paths from Uruguayan government sources. These establish pre-breach scope and are critical for regulatory disclosure scoping.

Step 2: Detection — Monitor threat intelligence feeds, dark web monitoring platforms, and paste sites for samples of the claimed dataset. Search for Uruguayan national ID patterns (Cédula de Identidad format) or government domain indicators in your inbound data flows. Review logs for anomalous API query volumes against any government-facing integrations. Apply AU-6 (Audit Record Review, Analysis, and Reporting) to examine access logs for data repositories holding Uruguayan citizen records. Behavioral indicator: bulk data export or query activity against citizen identity databases at unusual hours.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlate indicators from multiple sources; analyze anomalous access patterns against citizen PII repositories

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use free threat intelligence sources to search for leaked Cédula de Identidad samples: query IntelX (intelligence.x) and Have I Been Pwned's domain search for *.gub.uy. Write a YARA rule targeting 7-8 digit Uruguayan ID patterns co-located with Spanish-language PII fields (nombre, apellido, departamento) and run against any locally cached data samples. For log analysis without SIEM, use PowerShell against Windows application/security event logs: `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4663} | Where-Object {$_.Message -match 'citizen|cedula|uruguay'}` to surface unusual object access. For Linux database servers, parse PostgreSQL/MySQL slow query logs and general logs for SELECT * or LIMIT-less queries against citizen tables during off-hours (grep 'SELECT' /var/log/mysql/general.log | awk '{print $1,$2}' to extract timestamps).

Evidence: Preserve before any log rotation or system changes: (1) web server or API gateway access logs (Apache/NGINX access.log, IIS logs) showing query volume spikes to identity verification endpoints, filtered for *.gub.uy referrers or Uruguayan IP ranges (LACNIC-assigned blocks); (2) database audit logs capturing bulk SELECT operations against citizen PII tables — specifically queries returning >1000 rows or lacking WHERE clauses; (3) DNS query logs for outbound resolution of *.gub.uy domains at unusual hours, indicating automated exfiltration staging; (4) paste site or dark web monitoring alerts containing Cédula de Identidad number ranges matching your organization's known data holdings.

Step 3: Eradication — If your organization hosts or mirrors Uruguayan government data, audit access control configurations immediately against AC-3 (Access Enforcement) and AC-6 (Least Privilege). Revoke unnecessary API keys, service accounts, or external access grants touching citizen PII repositories. Rotate credentials for any accounts with read access to affected data stores per D3-CRO (Credential Rotation). Apply D3-UAP (User Account Permissions) to restrict data repository access to verified, role-justified accounts only.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Remove threat actor access paths, revoke compromised credentials, and verify unauthorized access grants are eliminated from citizen PII repositories

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without PAM tooling, enumerate all service accounts and API keys with access to citizen PII databases manually: on Linux, run `grep -r 'DB_PASSWORD\|API_KEY\|CEDULA' /etc/` and application config

directories to find embedded credentials; on Windows, use `net user /domain` and `Get-ADServiceAccount -Filter *` to list service accounts, then cross-reference against your data inventory from Step 1. Immediately revoke API keys via vendor portals (e.g., AWS IAM console, Azure AD app registrations) for any integration touching Uruguayan identity data. Document each revoked credential with timestamp — this log constitutes your eradication evidence trail for regulatory purposes.

Evidence: Capture before revoking any credentials: (1) complete export of current IAM role assignments, API key metadata (creation date, last used timestamp, associated service), and service account ACL entries for citizen PII repositories — this establishes the pre-eradication access state; (2) database user privilege exports (`SHOW GRANTS` in MySQL; `\du` in PostgreSQL) to document which accounts held SELECT/EXPORT permissions on affected tables; (3) API gateway access logs showing the full request history for each key being revoked, preserving evidence of whether the key was used for bulk extraction prior to your detection.

Step 4: Recovery — Validate that access control changes are enforced and logged. Confirm MFA is active on all accounts with access to citizen PII repositories (CIS 6.3, CIS 6.5; D3-MFA). Review AU-9 (Protection of Audit Information) to ensure audit logs covering affected repositories are intact, tamper-evident, and retained per AU-11. Monitor for follow-on social engineering targeting employees with Uruguayan-origin credentials or contacts — this data class frequently fuels spear-phishing campaigns.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore systems to verified secure state, enforce reconstituted access controls, and monitor for follow-on exploitation leveraging exfiltrated Uruguayan citizen PII

Controls: NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 4.3 (Configure Automatic Session Locking on Enterprise Assets)

Compensating: Verify MFA enforcement without enterprise IAM tooling by auditing authentication logs directly: on Azure AD, run `Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0}` to identify accounts without MFA; for Google Workspace, use Admin Console > Security > Authentication > 2-Step Verification enrollment report. For log integrity without a dedicated SIEM, configure auditd on Linux log servers (`auditctl -w /var/log/auth.log -p wa`) to detect tampering. To detect spear-phishing follow-on using Uruguayan PII lures, deploy a Sigma rule on mail gateway logs detecting inbound emails referencing 'Cédula', 'Ministerio del Interior', or 'DGI Uruguay' in subject lines from external senders — these are high-fidelity indicators of PII-weaponized phishing specific to this breach.

Evidence: Before closing recovery phase: (1) screenshot or export of MFA enrollment status for all accounts with citizen PII repository access, timestamped post-enforcement, to document the recovery control state; (2) audit log integrity check output — run `sha256sum` against archived log files covering the breach detection window and store hashes in a write-protected location to satisfy AU-9 tamper-evidence requirements; (3) email gateway or proxy logs for the 30 days following breach public disclosure, filtered for inbound messages referencing Uruguayan government entities or Cédula de Identidad terminology, establishing whether spear-phishing follow-on occurred.

Step 5: Post-Incident — Conduct a control gap review focused on CWE-284 and CWE-200: audit all externally exposed APIs and database interfaces for missing authentication, authorization enforcement, and rate limiting. Evaluate whether your organization's data minimization practices align with CIS 3.3 (Configure Data Access Control Lists) and CIS 3.4 (Enforce Data Retention). Brief third-party vendors processing Uruguayan citizen data on the breach claim and request their exposure assessments. Document findings for regulatory reporting purposes where applicable under data protection obligations.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned review, control gap remediation, regulatory documentation, and intelligence sharing with third-party vendors processing affected citizen PII

Controls: NIST SI-2 (Flaw Remediation), NIST CA-7 (Continuous Monitoring), NIST IR-4 (Incident Handling), NIST PM-14 (Testing, Training, and Monitoring), CIS 3.3 (Configure Data Access Control Lists), CIS 3.4 (Enforce Data Retention), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Audit externally exposed APIs for CWE-284 (Improper Access Control) and CWE-200 (Exposure of Sensitive Information) without commercial tooling: use OWASP ZAP in active scan mode against your identity verification API endpoints, specifically testing for unauthenticated access to citizen record endpoints and absence of rate limiting (send >100 requests/minute and verify 429 responses are returned). For data minimization gap analysis under CIS 3.3 and 3.4, query your database schemas directly: `SELECT table_name, column_name FROM information_schema.columns WHERE column_name LIKE '%cedula%' OR column_name LIKE '%national_id%'` to identify all tables retaining Uruguayan identity fields, then validate each against documented retention justification. Use this output as your vendor briefing evidence package.

Evidence: For regulatory documentation and lessons learned: (1) the complete data inventory output from Step 1 cross-referenced against the breach claim's reported data fields (full name, Cédula number, address, date of birth) — this scope comparison is required for breach notification threshold assessment under applicable data protection law; (2) OWASP ZAP scan reports or manual API audit results documenting CWE-284/CWE-200 findings against your government-facing integrations; (3) written vendor exposure assessment responses received in reply to your breach notification outreach, timestamped — these constitute due diligence evidence for regulatory purposes; (4) the access control change log from Steps 3 and 4 as the remediation record supporting any regulatory disclosure.

Detection Guidance

No confirmed IOCs are available; the breach claim originates from an RSS-aggregated source and has not been verified by CERTuy or Uruguayan government authorities. Detection should focus on behavioral and data-pattern indicators. (1) Dark web and paste site monitoring: search for sample data containing Uruguayan national ID (Cédula) format, 7-8 digit numeric strings associated with Uruguayan demographic fields. (2) Inbound data abuse: if your organization uses Uruguayan government identity data for verification, monitor for sudden spikes in identity match attempts using records that should not be in circulation. (3) Log review per NIST SP 800-53 AU-6: examine access logs on citizen data repositories for bulk SELECT queries, large result set exports, or API calls from unexpected source IPs, particularly outside business hours. (4) Threat intelligence correlation: map T1213 (Data from Information Repositories) and T1530 (Data from Cloud Storage) detection rules in your SIEM against Uruguayan government-connected data stores. (5) Social engineering precursor activity: the stolen PII class (identity, contact, demographic) is high-value for spear-phishing construction; increase scrutiny on inbound emails referencing Uruguayan government entities or officials targeting your staff. Validate any claimed breach dataset against official CERTuy disclosures before treating samples as confirmed. Note: URL verification for CERTuy's official breach notification portal is recommended pending confirmation of the primary reporting channel.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1041** — Exfiltration Over C2 Channel
- **T1078** — Valid Accounts
- **T1657** — Financial Theft
- **T1567** — Exfiltration Over Web Service
- **T1530** — Data from Cloud Storage
- **T1589.002** — Email Addresses
- **T1213** — Data from Information Repositories

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1657	Financial Theft	Impact
T1567	Exfiltration Over Web Service	Exfiltration
T1530	Data from Cloud Storage	Collection
T1589.002	Email Addresses	Reconnaissance
T1213	Data from Information Repositories	Collection

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/latin-americ...	T3
Uruguay Country Security Report - OSAC	https://www.osac.gov/Content/Report/559162b4-2baa-41f6-85d4-1d10cec...	T1
URUGUAY TARGETS CYBER SECURITY	https://www.trade.gov/market-intelligence/uruguay-targets-cyber-sec...	T1
2024 Trafficking in Persons Report: Uruguay - State Department	https://2021-2025.state.gov/reports/2024-trafficking-in-persons-rep...	T1
Susan Segal: Uruguay Shows the Power of a Sense of Security	https://www.americasquarterly.org/article/susan-segal-uruguay-shows...	T3

Generated 2026-05-27 18:54 UTC by TJS Security Command Center