National Civil Service Commission of Colombia Data Breach Exposes 2.9 TB of Government Files

By Written by

Published: 2025-11-11 · Archived: 2026-04-05 14:27:24 UTC

The National Civil Service Commission of Colombia data breach has exposed nearly 3 terabytes of government files following a cyberattack claimed by the Kazu ransomware group. The attackers listed the Comisión Nacional del Servicio Civil (CNSC) on their dark web leak portal, demanding a $300,000 ransom to prevent the disclosure of stolen data. The breach represents one of the largest confirmed government data exfiltrations in Latin America this year, with over 9 million files allegedly compromised.

Dark Web Monitoring

Background of the Breach

The National Civil Service Commission of Colombia (CNSC) is a critical government body responsible for overseeing recruitment, selection, and employment management for public sector workers across the country. Its mission ensures that hiring processes remain transparent and merit-based for civil service positions throughout Colombia. The organization’s official portal, https://cnsc.gov.co/, provides information on job openings, application procedures, and regulations governing public service employment.

According to the dark web listing, the Kazu threat group claimed to have successfully infiltrated CNSC’s network and exfiltrated 2.9 terabytes of sensitive data. The files reportedly contain internal communications, employee databases, application records, and government correspondence. The ransom note posted alongside the listing demanded $300,000 in exchange for deleting the stolen data, with a public disclosure deadline set for November 26, 2025.

About the Kazu Threat Group

Kazu is a relatively new but active cybercrime group that has surfaced on dark web marketplaces and leak sites since mid-2025. The group is known for targeting government and educational institutions in Latin America, Europe, and Asia. Kazu’s tactics resemble those of other double-extortion ransomware operators, where both data encryption and exfiltration are used to maximize leverage against victims. The group’s leak portal lists multiple ongoing ransom cases, with each victim assigned an expiration timer for ransom payment before public exposure.

Data Protection Services

In the case of CNSC, Kazu did not immediately publish evidence packs, suggesting negotiations or a delayed leak schedule. However, metadata from the listing confirms the presence of compressed archives totaling 2.9 TB and over 9.2 million records. This makes it one of the largest government data exfiltration incidents in Colombia’s history.

Scope of Exposed Data

Based on the information shared by the attackers, the **National Civil Service Commission of Colombia data breach** may have compromised:

- Employee and applicant personal records, including identification numbers, emails, and addresses
- Internal documents and correspondence between CNSC departments
- Government application forms and recruitment test results
- Financial records, payroll data, and contracts with civil service agencies
- System logs and configuration files from internal networks

The potential exposure of personal and governmental data could have serious implications for Colombia's public sector. Sensitive information such as ID numbers and job application histories can be exploited in identity theft, phishing, or political espionage campaigns. Moreover, the leak of internal procedures and recruitment materials could undermine public trust in the integrity of government hiring systems.

Impact on the Colombian Government

The incident raises major concerns for national data protection, as CNSC manages recruitment for thousands of government roles. If confirmed, the breach would represent a significant compromise of national personnel data. Public sector employees could face increased cyber risks, including credential-based attacks or targeted social engineering campaigns aimed at government departments.

In recent years, Latin American public institutions have become prime targets for ransomware groups due to a combination of valuable data, limited cybersecurity budgets, and the critical nature of public services. Similar large-scale attacks have previously targeted government agencies in Chile, Argentina, and Mexico, causing widespread operational disruptions and forcing major data restoration efforts.

Technical Aspects and Attack Vector

The method used by Kazu to infiltrate CNSC remains unknown, but the group commonly exploits weak remote desktop configurations, unpatched software vulnerabilities, and credential reuse across government systems. Analysts believe the group used phishing or stolen credentials to gain initial access, followed by lateral movement and data exfiltration over encrypted channels. The stolen files were reportedly compressed into multiple encrypted archives before being uploaded to private servers controlled by the attackers.

Home Network Security

The leak page listed both the ransom demand and publication timer, a standard feature of Kazu's extortion model. The 14-day countdown from the initial listing places the expected data release date on November 26, 2025, if no payment is made.

Comparative Context and Global Parallels

This breach bears resemblance to other high-profile ransomware attacks against government entities that combined data theft with extortion. It mirrors aspects of the Knownsec data breach and other international cases where stolen state data was used to pressure national authorities. Like those events, the CNSC attack demonstrates how cybercriminals increasingly target administrative systems managing civil infrastructure rather than focusing solely on commercial or financial sectors.

The size of the breach (nearly 3 terabytes) suggests full system infiltration, rather than selective data theft. The stolen information likely includes records that could be cross-referenced with national ID databases and tax records, amplifying privacy risks for millions of Colombian citizens.

Mitigation Strategies and Immediate Actions

For the National Civil Service Commission of Colombia

- Immediately disconnect affected servers and secure all endpoints to prevent further data exfiltration.
- Initiate a full forensic investigation to determine the entry vector, data scope, and systems impacted.
- Notify affected individuals and employees in accordance with Colombia's data protection laws.
- Engage with national cybersecurity authorities (ColCERT) and law enforcement agencies to coordinate incident response.
- Reset all credentials and implement multi-factor authentication across all CNSC systems.
- Review and strengthen network monitoring and backup policies to ensure resilience against similar attacks.

For Colombian Citizens and Public Sector Employees

- Be cautious of phishing messages impersonating CNSC or other government agencies.
- Monitor personal accounts for unusual login attempts or identity misuse.
- Update passwords for any government or recruitment-related accounts.
- Enable multi-factor authentication and regularly review security settings.
- Run system scans using a trusted anti-malware solution such as Malwarebytes to detect possible infections.

Wider Implications for Latin America

The Kazu ransomware group's focus on Latin American targets highlights growing cybercrime activity in the region. Government entities managing public databases have increasingly become entry points for cybercriminals due to outdated IT infrastructure and inconsistent data protection practices. As ransomware operations evolve, cooperation among Latin American cybersecurity agencies will be vital to strengthen defenses and improve early-warning systems for public sector networks.

Data Protection Services

For Colombia, the breach may trigger increased scrutiny of data security practices and legal reforms aimed at strengthening digital sovereignty. Similar to European data protection frameworks, Colombia may consider enhanced oversight mechanisms for government data storage and third-party software contracts.

Data Breach Summary

- **Organization:** National Civil Service Commission of Colombia (CNSC)
- **Location:** Colombia
- **Threat Actor:** Kazu ransomware group
- **Ransom Demand:** $300,000
- **Data Volume:** 2.9 TB (9,252,093 files)
- **Sector:** Government
- **Attack Type:** Ransomware and data exfiltration
- **Status:** Ongoing, data pending release

The National Civil Service Commission of Colombia data breach is a significant event in Latin America's cybersecurity landscape. The exposure of massive government records could have long-lasting implications for national data governance and citizen privacy. Strengthening digital infrastructure, improving access controls, and enhancing cross-agency threat intelligence will be crucial for preventing similar incidents in the future.

Home Network Security

For verified coverage of major data breaches and the latest cybersecurity threats, visit Botcrawl for ongoing updates and expert analysis on global digital security events.

Source: https://botcrawl.com/national-civil-service-commission-of-colombia-data-breach/