**Research Report:**

**NADRA Data Breach and Citizen Data Exposure**

**Presented By:**

**Javeria Anis**

**Date of Submission: 6th August, 2025**

Contents

[NADRA Data Breach and Citizen Data Exposure 3](#_Toc205397140)

[**1. Nature of the Leak** 3](#_Toc205397141)

[1. Supply‑Chain Vulnerabilities Exploited 3](#_Toc205397142)

[Router Compromise 3](#_Toc205397143)

[ISP-Level Risks 3](#_Toc205397144)

[2. Exploitation Techniques & Tools Used 3](#_Toc205397145)

[Insider Collusion 4](#_Toc205397146)

[Public API Misuse (PITB Portal) 4](#_Toc205397147)

[3. Leaked Data is still Available: 4](#_Toc205397148)

[4. Nature of the Leak (Explained via CIA Triad) 5](#_Toc205397149)

[Confidentiality 5](#_Toc205397150)

[5. Conclusion: 5](#_Toc205397151)

# NADRA Data Breach and Citizen Data Exposure

**1. Nature of the Leak**

The NADRA data breach involved unauthorized access to Pakistan’s national citizen database. This resulted in the leakage of sensitive personal information such as CNIC numbers, names, family tree data, addresses, and in some cases, associated mobile SIM information. The leaked data appears to originate from integrated databases linked with NADRA, such as telecom services and third-party government portals like the *Punjab AgriLoan* system.

The breach is believed to have occurred through **supply chain vulnerabilities**, particularly via external systems connected to NADRA through insecure APIs or leaked credentials. The exposed data is still accessible on some third-party websites, many of which allow form-based CNIC lookups and return full details.

## 2. Supply‑Chain Vulnerabilities Exploited

### Router Compromise

* Investigators concluded that the breach began with a **compromise of a PTCL router** inside a NADRA facility in Multan. This router was deployed as part of routine connectivity but had insufficient security configuration and network segmentation, granting attackers a persistent foothold into internal systems.
* According to a Biometric Update source, the attack began as early as **2016**, though it was publicly confirmed in March **2023**.

### ISP-Level Risks

* Independent analysts have warned that ISPs like PTCL often lack stringent control over deployed customer‑side equipment. Compromised routers or modems can be leveraged to intercept or reroute internal traffic.
* Reddit users echo the sentiment that compromised PTCL‑issued devices—once inside the local exchange—can be used to tap into broader networks.

**In a nut shell I would say that the** the root vulnerability was improper security hardening and insufficient monitoring of outsourced or third‑party network devices.

## 3. Exploitation Techniques & Tools Used

* The exact malware wasn’t spacified that what exactly was used but based on the evidences it is quite clear that athe attackers have used such kind of soctwares as listed below:
  + **Custom scripts or firmware backdoors** embedded in the router,
  + **Command‑and‑Control (C2) channels** for remote access,
  + **Insider‑driven operational support** to piece the data‑exfiltration methodology together.

### Insider Collusion

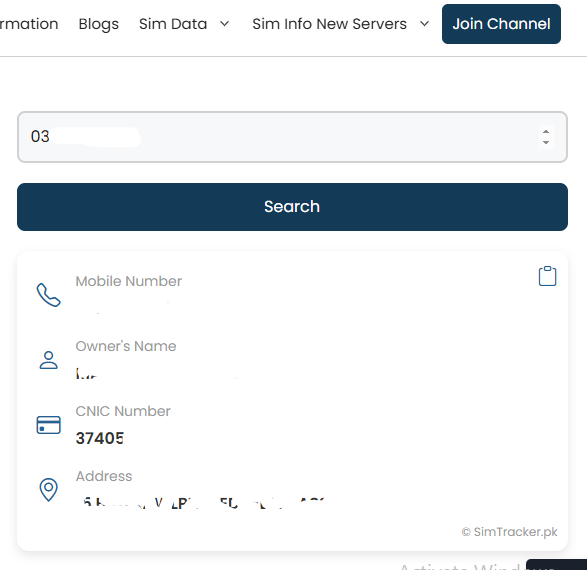
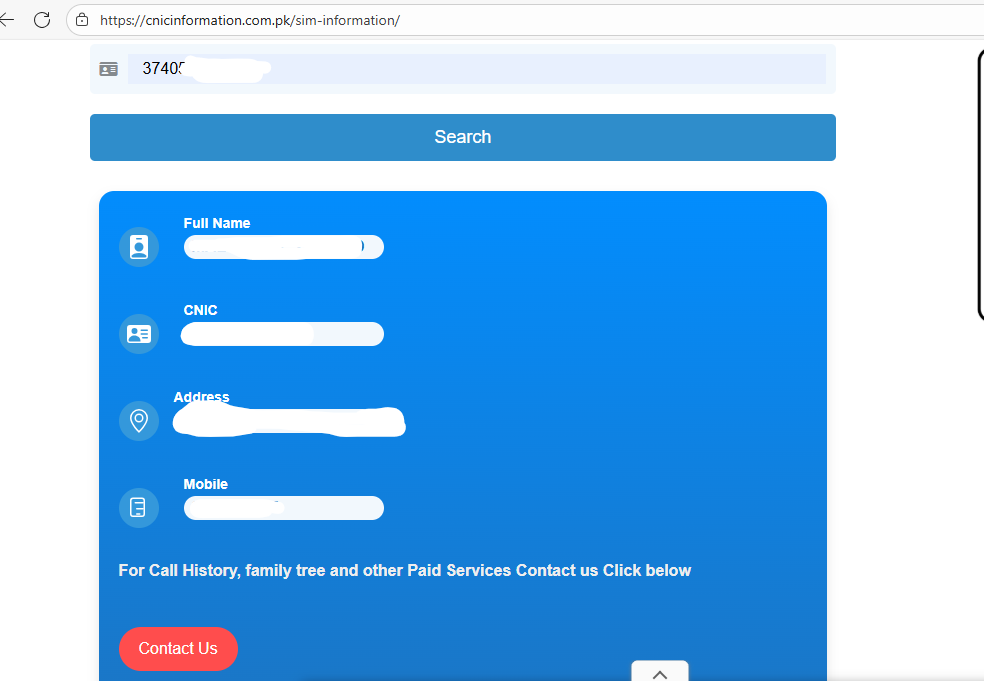
* The attack appears to have leveraged **privileged internal access**: insiders at multiple NADRA offices reportedly colluded with attackers to exfiltrate the stolen data. At least one Grade‑19 official was involved, and several internal credentials were likely misused.

### Public API Misuse (PITB Portal)

* Another angle of exposure came through the **Punjab Information Technology Board (PITB)**, which used NADRA-issued API keys in applications like AgriLoan.
* These credentialed portals lacked proper audit logs and access controls, meaning data could be programmatically extracted using simple scripts or UI automation tools (e.g. bots), even with shared public credentials.

## 4. Leaked Data is still Available:

While doing research on this topic I found out that people even with low knowledge can also gain knowledge about someone’s personal info like contact details, home address, family tree and even CNIC, which is a great threat to personal security and data piracy.



Having this information online can lead to ideantity theft and other challenges.

Another thing that I found was that older sims issued before 2023, their information was leaked but those after that are nor publicly available online on websites for public use. So we can say that the vulnerability has been overcomed to some extent but not as a whole. More steps need to be taken to protect users data from illegal use.

## ****5. Nature of the Leak (Explained via CIA Triad)****

The NADRA data breach exposed highly sensitive personal information of Pakistani citizens, such as:

* Full names
* CNIC numbers
* Family tree data
* Mobile numbers
* Addresses

This data was allegedly extracted from both NADRA’s core systems and third-party integrations (e.g., telecom companies, government portals like AgriLoan Portal, etc.).

### **Confidentiality**

**It was violated**: The breach directly compromised the confidentiality of citizens’ data. Personally identifiable information (PII) was leaked online, making private details publicly accessible on various third-party websites.

Even the officials have reported that “NADRA has been hacked twice… someone making the leaked database accessible online.”  
“There’s actually an API that you can use to get all this data… The API was publicly accessible and even usable from outside Pakistan.”

The integrity and Availability were not compromised because this wasn’t the main purpose of the attacker they wanted to steal the data and make it available online in which they succeeded.

## 6. Conclusion:

The NADRA data breach exposed serious weaknesses in Pakistan’s digital security. It compromised the confidentiality of citizens’ personal data, potentially affected data integrity, and revealed vulnerabilities that could threaten future system availability. Attackers exploited weak third-party systems and insecure APIs to access NADRA-linked information. The breach highlights the urgent need for stronger access controls, encryption, real-time monitoring, and better cybersecurity practices across all connected platforms. Overall, it reflects a major lapse in digital trust and national data protection.