EC THREATENED WITH LAW SUIT

By Abdulhaq Ibrahim

Seargent Alolga Akatapore, member of the erstwhile Provisional National Defense Council (PNDC) has threatened to sue the Electoral Commission (EC) if it fails to immediately take down its Web-Based Verification System.

In a letter to Madam Jean Mensa, the Chairperson of the Electoral Commission dated December 17, 2024, Seargent Akatapore urged the EC to temporarily disable the system untill the vulnerability has been adequately addressed.

The full text of the letter is published below;

Alolga Akata-Pore
E:aporelolga@proton.me
M:0263149776
17th December 2024

Madam Jean Mensa
The Chairperson
Electoral Commission of Ghana
EC Headquarters
Accra, Ghana

Subject: Urgent Notification of IDOR Vulnerability in the EC's Web-Based Voter Verification System

Dear Madam Jean Mensa,

I hope this letter finds you well. I am writing to bring to your immediate attention a critical Insecure Direct Object Reference (IDOR) vulnerability in the Electoral Commission's (EC) web-based voter verification system. This issue exposes the personal data of registered voters, including full names, voter ID numbers, dates of birth, polling station details, and photographs. Given the significance of this flaw, I respectfully urge immediate action to protect voters' sensitive data and restore confidence in the EC's systems.

Description of the Vulnerability

The EC's web-based voter verification tool allows users to input voter registration numbers to retrieve their registration details. However, the system fails to authenticate the enquirer or limit access appropriately. As a result:

1. Anyone with a valid voter registration number, whether obtained legally or otherwise can retrieve sensitive information belonging to other registered voters.
2. The returned data includes personal details such as full names, dates of birth, and polling station assignments, alongside the photographs of voters.

What makes this issue even more baffling is the timing of the app's deployment. The system was deployed after the 2024 elections (it first appeared on the 8th of December 2024), a period during which such functionality served no essential purpose. Its release raises serious questions about the rationale for its existence and further highlights lapses in oversight regarding the EC's IT infrastructure.

Furthermore, the system includes a button that allows users to make additional voter registration queries with minimal effort, further exposing a troubling lack of security awareness. By enabling users to repeatedly retrieve sensitive voter data without any form of authentication, the system essentially invites mass exploitation.

ATM or Momo Access Without a PIN

This vulnerability is akin to an ATM machine that does not require a PIN to access funds, or a Mobile Money App that allows transactions without requesting a security PIN. In either case, the absence of proper access controls would result in massive financial losses, as stolen or misplaced ATM cards and mobile phones could be easily misused. If any telecommunication company or bank deployed an application with such glaring flaws, it would face devastating consequences; lawsuits, regulatory fines, and a mass exodus of customers, leading to financial ruin. The fact that a system of such importance to our democracy operates with these vulnerabilities highlights a severe failure in implementing basic cybersecurity measures, undermining trust in the Electoral Commission and its IT systems.

This vulnerability mirrors the flaw previously identified in the EC's SMS-based verification system, which I notified your office about earlier this year.

Implications of the Vulnerability

While Ghanaian law permits the public exhibition of the voter register, access is traditionally restricted to specific periods and provided under controlled conditions to accredited political agents and stakeholders, whose activities are subject to oversight. The web-based system, however, bypasses these controls entirely by offering unrestricted and anonymous access to voter data. Unlike political agents, whose actions can be monitored and accounted for, anyone with internet access can now retrieve sensitive voter information without leaving a trace. This uncontrolled access compromises the EC's ability to determine who accessed its data and undermines the security and accountability mechanisms designed to protect voter privacy. The implications include:

1. **Identity Theft**: Malicious actors could use the data to impersonate voters or engage in fraud.
2. **Targeted Scams and Social Engineering**: Exposure of full names, dates of birth, and photographs makes it easier for scammers to manipulate voters through targeted messaging.
3. **Data Harvesting at Scale**: The lack of rate limits or security controls allows automated tools (bots) to collect data on thousands of voters in minutes.
4. **Erosion of Voter Trust**: Continued data exposures undermine public confidence in the EC's ability to secure electoral systems and protect personal information.
5. **Potential for Spoofing and Scams**

   The absence of authentication and unrestricted access to voter data in the EC's web-based verification system creates a significant opportunity for exploitation through spoofing and scams. Malicious actors can easily develop phishing websites that mimic the EC's official verification portal to deceive voters into providing sensitive personal information, such as registration numbers and

contact details. Such spoofed websites could then be used for identity theft, voter manipulation, or targeted scams.

This concern is not without precedent. During the deployment of the EC's SMS-based voter verification system, a simple typo in a widely published USSD code (*71151# instead of **711**51#) redirected users to an unrelated application seemingly offering financial products. While this error was swiftly corrected by the owners of the website which published the wrong USSD code, it exposed the EC's failure to anticipate the risk of typosquatting, where similar-looking codes or websites are used to exploit unsuspecting users.

In the case of the web-based verification system, the risks are amplified because

- More personal voter data, including full names, dates of birth, and photographs, are exposed.
- Access is entirely **anonymous** and uncontrolled, meaning the EC cannot determine **who** queries the system or for what purpose.
- Spoofed or cloned websites are harder for voters to distinguish, given the open nature of internet access

A Broader Issue: Data Security and System Oversight

This situation highlights significant lapses in the EC's cybersecurity and data management protocols. Contractors responsible for this system may have developed other EC systems, raising concerns that similar vulnerabilities exist elsewhere within the EC's IT infrastructure. Additionally, the persistence of this flaw raises questions about whether appropriate audits, vulnerability assessments, and quality assurance measures are being implemented.

Immediate Recommendations

To mitigate the risks posed by this vulnerability, I respectfully recommend the following immediate actions:

1. Take Down the Web-Based Verification System: Temporarily disable the system until the vulnerability has been adequately addressed.
2. Notify Affected Voters: Inform registered voters of this data exposure and issue an unreserved public apology for any risks caused by the flaw.
3. Secure the System: Implement industry-standard security measures, including authentication controls, rate limiting, and data encryption.
4. Commission a Full Audit: Conduct a comprehensive security audit of all EC systems to identify and address similar vulnerabilities.

Next Steps

Given the seriousness of this vulnerability and its implications for voter data security, I respectfully request that immediate steps be taken to disable the system and resolve

the issues highlighted. Should no action be taken within the next seven (7) days, I will be left with no choice but to pursue appropriate legal remedies to compel the EC to secure this critical system and protect the personal data of Ghanaian voters.

My sole aim is to ensure that the integrity of the EC's systems is preserved and that public trust in our electoral processes is strengthened. I remain available to collaborate or provide further details to assist in addressing these critical concern

Please find attached a summary article detailing the vulnerability and its broader implications for the public interest.

Yours sincerely

Alolga Akata-Pore

CC:

The Data Protection Commissioner
The Minister of National Security