CRITICAL INFRASTRUCTURE SUBSECTOR	Election Systems
SUBJECT	Decryption Keys
COMPONENT SCOPE	Election Management Systems
RISK LEVEL	High
ELECTION RECORDS IMPACTED	Voter Registration Information Ballot Designs and Configurations Vote Tallies and Results

1 Introduction

Storing decryption keys in plain text creates a major security vulnerability. If an attacker gains access to the database, they could easily obtain the keys and use them to decrypt sensitive election data such as voter registration information, ballot designs and configurations, and vote tallies and results.

2 Background

The Lake v Fontes lawsuit before the Supreme Court of the United States introduced a significant body of evidence regarding security vulnerabilities found in the Election Management System (EMS) developed by Dominion Voting Systems.

No. 23-1021

In the Supreme Court of the United States

KARI LAKE AND MARK FINCHEM,
Applicants,
v.
ADRIAN FONTES, ARIZONA SECRETARY OF STATE, *ET. AL.*,
Respondents.

On Petition for Writ of *Certiorari*
to the U.S. Court of Appeals
for the Ninth Circuit

APPENDIX TO PETITIONERS' MOTION TO EXPEDITE

KURT B. OLSEN
Olsen Law PC
1250 Connecticut Ave. NW
Suite 700
Washington, DC 20036
202-408-7025
ko@olsenlawpc.com

LAWRENCE J. JOSEPH
Counsel of Record
1250 Connecticut Ave. NW
Suite 700
Washington, DC 20036
202-355-9452
ljoseph@larryjoseph.com

Patrick M. McSweeney
McSweeney, Cynkar & Kachouroff PLLC
3358 John Tree Hill Road
Powhatan, VA 23139
804-937-0895
patrick@mck-lawyers.com

Counsel for Petitioners

One of the most concerning discoveries of cybersecurity expert Ben Cotton upon examination of EMS images used in Maricopa County, AZ during the 2020 and 2022 elections pertains to the storage of encryption and decryption keys within the EMS election database. In Mr. Cotton's sworn testimony, her states the following:

"The DVS Democracy Suite utilizes a combination of a Rjindael Key, a Rjindael Vector, a Hash-based Message Authentication Code (HMAC) and a x509 security certificate to encrypt, decrypt and authenticate data. This data includes code signing, data signing, communications, and tabulator results from ICC or ICP2 components. The protection of election encryption and decryption keys is prominently described by DVS within Democracy Suite Technical Data Package documents as the mitigation for the risk fo a malicious actor tampering with the election database, election result files, scanned ballot images, device audit logs, device log reports, ballot definitions and other critical elements that could allow authorized or unauthorized parties, to alter the outcome of an election without detection. These keys have been left unprotected on the election database and are in plain text as shown below:

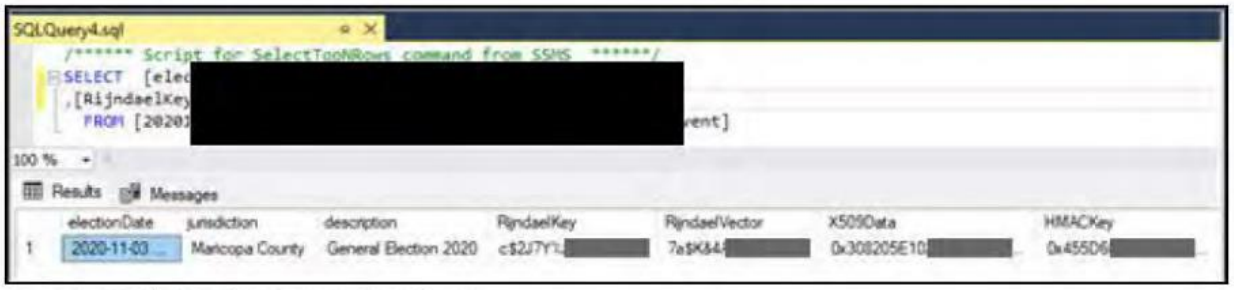

Figure 7 - Rijndael Key for Maricopa 2020 Election

The only barrier to access these keys is the Windows-login. This login obviously would not prevent a malicious insider from changing results. A non-insider could easily bypass the Windows Login feature in about 5 minutes with well-known hacking techniques available on the internet. Given the cyber security vulnerabilities, including the sharing of passwords between user accounts, access to all of these encryption elements is easily obtained. The encryption elements are stored in the MS SQL election database and are easily retrieved with a simple SQL query."

3 Impact

3.1 Election Record Tampering

With decryption keys exposed, malicious actors could potentially:

- Access and modify voter rolls
- Tamper with ballot definitions
- View or alter vote counts before official release

This undermines the confidentiality and integrity of the entire election process

3.2 Loss of Public Trust

If it became public knowledge that decryption keys were improperly secured, it would likely lead to:

- Decreased voter confidence in the election system
- Questions about the validity of results
- Potential legal challenges to election outcomes

Maintaining public trust is critical for democratic election

3.3 Violation of Security Standards

Storing encryption keys in plain text violates basic cybersecurity best practices and likely contravenes:

- Federal and state election security guidelines
- Data protection regulations
- Industry standards for key management

This could result in compliance issues and potential penalties

4 Risk Mitigation Strategy

If state law permits the removal of electronic voting systems, election officials should:

- Remove electronic voting systems
- Define and implement hand count procedures
- Maintain local voter rolls on equipment that is not connected to the internet

If state law mandates the use of electronic voting systems, election officials should:

- Use proper key management systems to securely store and manage encryption keys
- Implement strong access controls and authentication for election databases
- Conduct regular security audits to detect vulnerabilities
- Follow NIST guidelines for protecting sensitive election data

Proper encryption and key management are essential for maintaining the security and integrity of electronic voting systems. Any discovery of improperly stored keys should be treated as a serious security incident requiring immediate remediation.

5 Conclusion

The storage of decryption keys in plain text without electronic voting systems presents a significant risk to the integrity of our elections. If your organization does not have sufficient cybersecurity expertise to identify and mitigate such risks, either obtain such skills from trusted resources within your organization or advocate for a return to manual systems that do not require such expertise in order to conduct elections in a secure manner.