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

1 Introduction

Maintaining the integrity and security of electronic voting systems requires strict adherence to certified configurations and security protocols. Any deviations should be carefully evaluated and approved through proper channels to ensure they do not compromise the system's security or certification status.

2 Background

The Help America Vote Act (HAVA) mandates that the Election Assistance Commission (EAC) accredit voting system test laboratories and certify voting equipment.

2.1 Certified Voting Systems

The EAC website maintains a list of Certified Voting Systems. For each certified system, the EAC provides a list of hardware and software components associated with the certification.

2.2 MS SQL Server Management Studio

Despite not being listed by the EAC as a software component for a certified Dominion Voting System (DVS) configuration, Microsoft SQL Server Management Studio (SSMS) has been found installed on Election Management System (EMS) servers in the following communities as a minimum: Antrim County, MI[1], Mesa County, CO[2], and Canton Township, MI[3].

2.3 Compiler

The Dominion EMS installation examined in Maricopa County, AZ revealed the existence of a compiler installation. The compiler "provides the ability to modify and create executable files and drivers on the fly that could be used to alter election results without detection."[4]

3 Impact

Installing non-certified software like Microsoft SQL Server Management Studio and a compiler onto an Election Management System (EMS) server for an electronic voting system poses several significant security risks:

[1] https://www.michigan.gov/-/media/Project/Websites/sos/30lawens/Antrim.pdf?rev=fbfe881cdc0043a9bb80b783d1bb5fe9

[2] https://letsfixstuff.org/2023/04/what-evidence-do-we-have-of-electronic-voting-system-vulnerabilities/

[3] https://letsfixstuff.org/2023/05/canton-mi-detroit-not-the-only-municipality-covering-up-elections-gross-negligence/

[4] Expert testimony of Ben Cotton in Lake v Fontes, https://lindelloffensefund.org/wp-content/uploads/2024/03/Lake-Mot-to-Expedite-App-filed.pdf

3.1 Increased Attack Surface

Adding unauthorized software expands the potential attack surface of the EMS server[5,6]. This introduces new vulnerabilities that could be exploited by malicious actors to compromise the integrity of the voting system.

3.2 Violation of Certification Requirements

Electronic voting systems undergo rigorous certification processes to ensure security and reliability[7,8]. Installing non-certified software likely violates these requirements, potentially invalidating the system's certification and compromising its trustworthiness.

3.3 Unauthorized Access and Manipulation

Tools like SQL Server Management Studio could potentially allow unauthorized access to and manipulation of election databases[9,10]. A compiler introduces the risk of malicious code being developed and executed on the EMS server.

3.4 Compromised System Integrity

Non-certified software may not meet the stringent security standards required for election systems[11,12]. This could lead to unintended system behavior, data corruption, or vulnerabilities that compromise the overall integrity of the voting process.

3.5 Audit Trail Complications

Unauthorized software installations complicate the audit trail and make it more difficult to verify the system's security and proper functioning[13,14]. This undermines transparency and accountability in the election process.

3.6 Increased Vulnerability to Malware

Additional software increases the risk of malware infection, potentially allowing attackers to manipulate vote counts or access sensitive voter information[15,16].

3.7 Chain of Custody Issues

Installing unauthorized software breaks the chain of custody and violates best practices for maintaining the security of election systems throughout their lifecycle[17,18].

[5] https://www.essvote.com/faqs/

[6] https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01

[7] https://www.essvote.com/faqs/

[8] https://www.eac.gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.pdf

[9] https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf

[10] https://www.cisa.gov/news-events/news/best-practices-securing-election-systems

[11] https://www.essvote.com/faqs/

[12] https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01

[13] https://www.cisa.gov/news-events/news/best-practices-securing-election-systems

[14] https://www.eac.gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.pdf

[15] https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf

[16] https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01

[17] https://www.cisa.gov/news-events/news/best-practices-securing-election-systems

[18] https://www.eac.gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.pdf

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:

- Strictly adhere to certified configurations
- Implement rigorous access controls
- Conduct regular security audits
- Use air-gapped systems where possible
- Follow proper chain of custody procedures

5 Conclusion

The installation of non-certified software like Microsoft SQL Server Management Studio and a compiler on Election Management System (EMS) servers in multiple jurisdictions represents a serious breach of voting system security protocols and certification requirements. This practice significantly compromises the integrity, security, and reliability of the affected electronic voting systems.

The widespread nature of these unauthorized installations across multiple jurisdictions suggests a systemic problem that requires immediate attention and corrective action to ensure the integrity of future elections.