Dominion Democracy Suite ImageCast Remote 5.2 RAVBMS Security and Telecommunications Test Report

DOM-18001-RSECTR-01

Prepared for:

Vendor Name	Dominion Voting
Vendor System	Democracy Suite ImageCast Remote 5.2

Prepared by:

4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

Accredited by the Election Assistance Commission (EAC) for Selected Voting System Test Methods or Services

Revision History

Date	Release	Author	Revision Summary
3.30.2018	v1.0	J. Peterson, M. Santos	Initial Release
4.10.2018	v1.1	M. Santos	Updates for CASOS comments

Disclaimer

The information reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government.

Trademarks

- SLI is a registered trademark of SLI Compliance.
- All products and company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

INTRODUCTION

The California Voting Systems Standards (CVSS) were written in such a way to be applicable to a wide variety of voting technology. Therefore, the relevant portions of the CVSS are reviewed as the relate to the Remote Accessible Vote By Mail (RAVBM) system for the purposes of this report. The use of "voting system" shall apply to the RAVBM system.

This report outlines the testing SLI Compliance (SLI) followed when performing Security and Telecommunications Testing on the **Dominion Democracy Suite ImageCast Remote 5.2 (RAVBM)** system (DS ICR 5.2 RAVBM system) against the California Voting System Standards (CVSS).

The DS ICR 5.2 RAVBM system enables the voter to mark their ballot using a secure web-based interface, and generate and download a PDF representation of choice selections. Voters then print that ballot, and then return it to their clerk.

Phase I – Documentation Review

During Phase I testing of the **Dominion DS ICR 5.2 RAVBMS** (DS ICR 5.2 RAVBM system), documentation was reviewed to verify and validate the following requirements:

- Top-level system design and architecture
- System documentation and procedures

During Phase I testing, documentation was reviewed to verify and validate in accordance with the following CVSS requirements:

- 5.5 Vote Secrecy on Direct Recording Electronic (DRE) and Electronic Ballot Marking (EBM) Systems
- 6.1.2 Data Transmissions
- 6.2 Design, Construction, and Maintenance Requirements
- 6.2.1 Confirmation
- 7.1.1 Elements of Security outside Manufacturers Control
- 7.2 Access control
- 7.2.1 General Access Control
- 7.2.2 General Access Control
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation
- 7.8 Testing – Security

See the applicable section below for more details on these requirements and the review results.

5.5 Vote Secrecy on DRE and EBM Systems

All DRE and EBM systems **shall** ensure vote secrecy by:

a. Immediately after the ballot is recorded to persistent electronic storage or printed, erasing the selections from the device's display, working memory, and all other storage, including all forms of temporary storage

b. Immediately after the voter chooses to cancel his or her ballot, erasing the selections from the display and all other storage, including buffers and other temporary storage

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

6.1.2 Data Transmissions

These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable:

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually

Ballot Definition: Information that describes to a voting machine the content and appearance of the ballots to be used in an election

Vote Count: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count

List of Voters: A listing of the individual voters who have cast ballots in a specific election

Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

6.2 Design, Construction, and Maintenance Requirements

Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities **shall** be considered basic to all data transmissions.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

6.2.1 Confirmation

Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission the user shall be notified of the action to be taken.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

7.1.1 Elements of Security outside Manufacturers Control

The requirements of this section apply to the capabilities of a voting system that must be provided by the manufacturer. However, an effective security program requires well defined security practices by the purchasing jurisdiction and the personnel managing and operating the system. These practices include:

- Administrative and management controls for the voting system and election management, including access controls
- Internal security procedures
- Adherence to, and enforcement of, operational procedures (e.g., effective password management)
- Security of physical facilities
- Organizational responsibilities and personnel screening

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

7.2 Access control

Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

Access controls may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security

software programs designed to prevent or detect unauthorized access to sensitive files. The access controls described in this section are limited to those controls required to be provided by system manufacturers.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

7.2.1 General Access Control

General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

a. Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.
    i. Access control mechanisms on the EMS **shall** be capable of identifying and authenticating individuals permitted to perform operations on the EMS.
b. Voting system equipment **shall** provide controls that permit or deny access to the device's software and files.
c. The default access control permissions **shall** implement the minimum permissions needed for each role or group identified by a device.
d. The voting device **shall** prevent a lower-privileged process from modifying a higher-privileged process.
e. An administrator of voting system equipment **shall** authorize privileged operations.
f. Voting system equipment **shall** prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

7.2.2 Access Control Identification

Identification requirements provide controls for accountability when operating and administering a voting system.

a. The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

7.4.5 Software Reference Information

a. The manufacturer **shall** provide the NSRL, any California certified escrow facility, pursuant to Title 2, Division 7, Chapter 6 of the California Code of Regulation, and the Office of the Secretary of State with a copy of the software installation disk, including the executable binary images of all third party software. Further, the manufacturer **shall** deposit the source code, tools, and documentation, to allow the complete and successful compilation of a system in its production/operation environment.

   i. The manufacturer **shall** document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.

c. The manufacturers **shall** document to whom they provide voting system software.

Results: Review of the Technical Data Package (TDP) determined the documentation doesn't describe a process used to verify the software distributed is the software provided by the NSRL or designated repository. The documentation doesn't provide a procedure or functionality to verify that the software is the certified software by comparison.

7.4.6 Software Setup Validation

g. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).

Results: Review of the Technical Data Package (TDP) determined the documentation doesn't reference any type of digital verification on software prior to installation. No documentation on the method provided by external interface or equipment used to verify software on the system. No documentation about a mechanism for detecting unauthorized software.

7.8 Testing – Security

The S-ATA **shall** design and perform test procedures that test the security capabilities of the voting system against the requirements. These procedures **shall** focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures **shall** also examine system capabilities and safeguards claimed by the manufacturer in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems **shall** be tested for effective access control and physical data security.

The S-ATA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the manufacturer must provide the published standards and methods used by the U.S. Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites.

At its discretion, the S-ATA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities.

7.8.1 Access Control

The accredited testing laboratory **shall** conduct tests of system capabilities and review the access control policies and procedures submitted by the manufacturer to identify and verify the access control features implemented as a function of the system. For those access control features built in as components of the voting system, the S-ATA **shall** design tests to confirm that these security elements work as specified.

Specific activities to be conducted by the S-ATA **shall** include:

a. A review of the manufacturer's access control policies, procedures and system capabilities to confirm that all requirements have been addressed completely

Results: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

Phase II – Functional Security Testing

Phase II testing included:

- Testing of relevant software and operating system configuration for pertinent vulnerabilities
- Testing of hardware, including examination of unused hardware ports and security measures applied to those ports

During Phase II, tests were exercised in order to verify and validate functional security in accordance with the following CVSS requirements:

- 5.5 Vote Secrecy on DRE and EBM Systems
- 7.2.1 General Access Control
- 7.2.2 Access Control Identification

- 7.2.4 Access Control Authorization
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation
- 7.6 Telecommunications and Data Transmission
- 7.8 Testing – Security
- 7.8.1 Access Control
- 7.8.2 Data Interception and Disruption

See the applicable section below for more details on these requirements and the review results.

An issue log of any errors, anomalies, or omissions encountered during Phase II testing was maintained.

5.5 Vote Secrecy on DRE and EBM Systems

All DRE and EBM systems **shall** ensure vote secrecy by:

a. Immediately after the ballot is recorded to persistent electronic storage or printed, erasing the selections from the device's display, working memory, and all other storage, including all forms of temporary storage

b. Immediately after the voter chooses to cancel his or her ballot, erasing the selections from the display and all other storage, including buffers and other temporary storage

Testing performed: Testing was performed to verify how the system handled a ballot being printed and the browser closed, as well as when the ballot is closed prior to being printed. Attempts were made to resume a ballot, as well as to determine if any ballot information resided in history or cache. Verified that no traces of marked ballot information existed in browser history or cache.

7.2.1 General Access Control

General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

a. Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.

Testing performed: The DS ICR 5.2 RAVBM system uses an N-tier architecture that consists of separate client applications, application server components, database components, and a central document repository.

Authentication included methods for both the voter facing application as well as the administrative application.

Security was tested on the architecture pieces, client application, and administrative application, which were accessible remotely.

Physical security was not able to be observed as this was hosted at a data center.

7.2.2 Access Control Identification

Identification requirements provide controls for accountability when operating and administering a voting system.

a. The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.

Testing performed: The DS ICR 5.2 RAVBM system uses a client server system to authenticate registered voters and serve up the correct ballot for a particular voter using predefined ballot rules and voters that can be imported by the jurisdiction.

Role based access controls are in place for administrative login purposes.

7.2.4 Access Control Authorization

a. Voting systems shall ensure that only authorized roles, groups, or individuals have access to election data.

b. Voting systems shall explicitly authorize subject's access based on access control lists or policies.

c. Voting systems **shall** explicitly deny subject's access based on access control lists or policies

Testing performed: All access to the DS ICR 5.2 RAVBM system is controlled by Voter ID number and an associated pin number which is created during registration.

All administrative access is controlled by username/password combinations and there is a role-based administrative access in place.

The ability to assign voters to different electoral groups/electoral districts gives the ability to assign ballots to voters in accordance with specific rules.

7.4.5 Software Reference Information

b. The voting system equipment **shall** be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.

Testing performed: No methods or procedures for verification if the system is running certified unmodified code were presented.

Testing was unable to successfully modify the server code to verify if a protection method was in place and viable.

7.4.6 Software Setup Validation

c. Setup validation methods **shall** include a software verification method that ensures that the voting system software has not been modified illegitimately.
   i. The voting systems **shall** include any supporting software and hardware necessary to conduct the software verification method.
   ii. The manufacturer **shall** document the process used to conduct the software verification method.
   iii. The software verification method **shall** not modify the voting system software on the voting system.

Testing performed: The DS ICR 5.2 RAVBM system does not have a built in hash verification method for the system which provides a method to verify that the source code is not running modified code.

Testing was unable to successfully modify the server code to verify if a protection method was in place and viable.

7.6 Telecommunications and Data Transmission

There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.

Testing performed: Tests were performed to verify that the system utilizes electrical or optical transmission, and that the ballot is sent via SSL and no receipt is utilized to verify. The client generates a blank ballot which does not contain voting selections. Once the blank ballot is delivered, and until the ballot package is saved, there are no external communications between the voter and the ballot delivery system; all interactions remain local to the voter's environment.

7.8 Testing – Security

The state-approved testing agency (S-ATA) **shall** design and perform test procedures that test the security capabilities of the voting system against the requirements. These procedures **shall** focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures **shall** also examine system capabilities and safeguards claimed by the manufacturer in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless

of system design and risk profile, all systems **shall** be tested for effective access control and physical data security.

The S-ATA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the manufacturer must provide the published standards and methods used by the U.S. Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites.

At its discretion, the S-ATA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities.

Testing performed: Confirmed that the DS ICR 5.2 RAVBM system does not have, nor require, internet access once the ballot has been downloaded. There are no external connections from the ballot to any outside server or service. With the exception of printing or saving the ballot package there are no external calls to or from the ballot.

7.8.1 Access Control

For those access control features built in as components of the voting system, the S-ATA **shall design tests to confirm that these security elements work as specified**.

Specific activities to be conducted by the S-ATA **shall** include:

b. Specific tests designed by the S-ATA to verify the correct operation of all documented access control procedures and capabilities, including tests designed to circumvent controls provided by the manufacturer. These tests **shall** include:

   i. Performing the activities that the jurisdiction will perform in specific accordance with the manufacturer’s access control policy and procedures to create a secure system, including procedures for software and firmware installation

   ii. Performing tests intended to bypass or otherwise defeat the resulting security environment. These tests **shall** include simulation of attempts to physically destroy components of the voting system in order to validate the correct operation of system redundancy and backup capabilities

This review applies to the full scope of system functionality. It includes functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote canvassing, vote reporting, and maintenance of the system’s audit trail.

Testing performed: Testing was performed to confirm that DS ICR 5.2 RAVBM system access control was maintained. Attempted XSS attacks, SQL Injection attacks, directory listings/scans, attempted to pull directory file lists, scanned for

default http login pages, scanned for robots_txt file, and pulled SSL certificate information.

A full WMAP Web vulnerability scan was performed.

Burp Suite was utilized to fully scan, spider, and intercept both the Voter facing application and the Administrative application.

A Nessus scan of the system was also performed.

Review of the requirement validated that the requirement was satisfactorily covered.

7.8.2 Data Interception and Disruption

For systems that use telecommunications, as provided for in section 6 of the Standards and consistent with California law, to transmit official voting data, the S-ATA **shall** review, and conduct tests of, the data interception and prevention safeguards specified by the manufacturer in its TDP. The S-ATA **shall** evaluate safeguards provided by the manufacturer to ensure their proper operation, including the proper response to the detection of efforts to monitor data or otherwise compromise the system.

Testing performed: Verified that this system does not utilize telecommunications for the transmission of official voting data; only for delivery of a blank ballot that does not contain voter data or choice selections.

Phase III – Telecommunications and Data Transmission Testing

Phase III consisted of the testing of system communications, including encryption of data, as well as protocols and procedures for access authorization

During Phase III, tests were exercised in order to verify and validate telecommunications and data transmission in accordance with the following CVSS requirements:

- 6.1.2 Data Transmission
- 6.2 Design, Construction, and Maintenance Requirements
- 6.2.1 Confirmation

See the applicable section below for more details on these requirements and the review results.

An issue log of any errors, anomalies, or omissions encountered during Phase III testing was maintained.

6.1.2 Data Transmission

These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable:

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually

Ballot Definition: Information that describes to a voting machine the content and appearance of the ballots to be used in an election

Vote Count: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count

List of Voters: A listing of the individual voters who have cast ballots in a specific election

Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section.

Testing performed: Web Vulnerability scans were performed on the DS ICR 5.2 RAVBM system web server to determine if there were any basic web server vulnerabilities in the initial serving of the in-browser application that houses the DS ICR 5.2 RAVBM system ballot.

After the interactive ballot application is launched, connectivity to and from the ballot were confirmed to be nonexistent, with the exception of calls to the local system for print functionality.

6.2 Design, Construction, and Maintenance Requirements

Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities **shall** be considered basic to all data transmissions.

Testing performed: Verified that DS ICR 5.2 RAVBM system consists of a generated ballot which is typically used for absentee and mail in ballot marking. The DS ICR 5.2 RAVBM system does not utilize specific telecommunications channels once the ballot has been downloaded and opened on the voter's machine.

6.2.1 Confirmation

Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission the user shall be notified of the action to be taken.

Testing performed: Testing verified that the DS ICR 5.2 RAVBM system ballot package only allows the voter to mark and confirm marked ballots prior to printing and or saving out a ballot package

There are no live connections from the application to a remote server after the voter receives the generated ballot.

All selections are cleared after the browser has been closed.

This requirement was determined to be not applicable.

Potential Vulnerabilities

For any potential vulnerabilities discovered, SLI was tasked with identifying the particular standards applicable to each vulnerability.

To the extent possible, reported vulnerabilities include an indication of whether the exploitation of the vulnerability would require access by a:

- Voter: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for less than an hour.
- Poll worker: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for up to one week, but all physical security has been put into place before the machines are received.
- Elections official insider: Wide range of knowledge of the voting machine design and configuration. May have unrestricted access to the machine for long periods of time. Their designated activities include:
  - Set up and pre-election procedures;
  - Election operation;
  - Post-election processing of results; and
  - Archiving and storage operations.

- Vendor insider: With great knowledge of the voting machine design and configuration. They have unlimited access to the machine before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service, and when providing election administration services.

SLI will not verify or demonstrate exploitability of the vulnerability but the report of the vulnerability will identify factors involved in the exploitation.

Any vulnerability theories developed by the security team shall, to the extent possible, be referred to the Secretary of State staff.

7.2.1 General Access Control

General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

a. Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.
    i. Access control mechanisms on the EMS **shall** be capable of identifying and authenticating individuals permitted to perform operations on the EMS.
b. Voting system equipment **shall** provide controls that permit or deny access to the device's software and files.
c. The default access control permissions **shall** implement the minimum permissions needed for each role or group identified by a device.
d. The voting device **shall** prevent a lower-privileged process from modifying a higher-privileged process.
e. An administrator of voting system equipment **shall** authorize privileged operations.
f. Voting system equipment **shall** prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.

On the administrative application it was found that the password field has autocomplete enabled, allowing the browser to cache and store passwords for future visits to the application. Stored credentials can be captured by an attacker if the user's computer is compromised.

For the vulnerability in question, the level of access required to take advantage of this potential vulnerability would be inclusive to the following actors:

- Election official insider, who could attempt to steal other's credential to access the administrative application in an unauthorized manner.
- Vendor Insider, who could attempt to steal other's credential to access the administrative application in an unauthorized manner.

7.4.5 Software Reference Information

a. The manufacturer **shall** provide the NSRL, any California certified escrow facility, pursuant to Title 2, Division 7, Chapter 6 of the California Code of Regulation, and the Office of the Secretary of State with a copy of the software installation disk, including the executable binary images of all third party software. Further, the manufacturer **shall** deposit the source code, tools, and documentation, to allow the complete and successful compilation of a system in its production/operation environment.

   i. The manufacturer **shall** document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.

b. The voting system equipment **shall** be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.

c. The manufacturers **shall** document to whom they provide voting system software.

No verification methods were provided to ensure that the server that provides the application to the voter to generate his/her ballots is running unmodified code.

For the vulnerability in question, the level of access required to take advantage of this potential vulnerability would be inclusive to the following actors:

- Voter, who can attempt to modify the server code remotely.
- Election official insider, who could attempt to modify the server code remotely.
- Vendor Insider, who could attempt to locally modify the server code.

7.8 Testing – Security

Target: www.uocava.com (Voter facing application)

- Potential Cross Site Scripting opportunity in select components of the system. (High Severity)
- Potential Instances of Cross site Request Forgery in select components of the System. (Medium Severity)

Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. For a request to be vulnerable to CSRF, the following conditions must hold:

- The request can be issued cross-domain, for example using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
- The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
- The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
- The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable

- Potential Open Redirection (DOM-Based) (Low Severity) may be a false Positive.

  DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

  DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

  Note: If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the JavaScript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

  Target: https://admin.uocava.com (Administrative portal)

- Potential instances of SQL Injection. (High severity)

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

- SSL Certificate Not trusted: (Medium Severity)

  This issue may just be an issue with the tool's Root CA Store not having a cloudFlare Trusted Root Certificate. It's suggested that the server use a certificate from a widely known and trusted Certificate authority.

  SSL (or TLS) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To achieve this, the server must present an SSL certificate that is valid for the server's hostname, is issued by a trusted authority, and is valid for the current date. If any one of these requirements is not met, SSL connections to the server will not provide the full protection for which SSL is designed.

- Potential Open Redirection (DOM-Based) (Low Severity) may be a false Positive.

  DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

  DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

  Note: If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the JavaScript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

- Password Field with Autocomplete enabled (Low Severity)

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

- Strict Transport Security not enforced (Low Severity)

  The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

  To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Summary

The DS ICR 5.2 RAVBM system is an application that allows voters to access ballots remotely as controlled by the jurisdiction. The ballot, once generated and accessed, is self-contained within the individual voter’s browser. This means that once the initial server call for the application is processed the entire application runs in the current browser session. Since the application doesn’t utilize incoming or outgoing connections once the ballot is loaded, this reduces the possibility of interception or manipulation through network attack vectors.

This, however, poses a risk of server side compromise. To help mitigate this, the vendor should provide high level documentation about the processes/procedures and security to mitigate these risks. Including but not limited to

- Secure hosting
- Physical security of hosting sites

- Network security
- Inventory and configuration management
- Access control
- Monitoring and logging

Security testing of the server side hosting security included application scanning, and Nessus vulnerability scanning. The results of this scanning turned up a small selection of High, Medium, and Low vulnerabilities that have minimal impact on the overall security of the applications being tested.

It was determined that the DS ICR 5.2 RAVBM system utilizes Cloudflare to serve the ballot. Cloudflare provides redundant DDOS Protection, DNS, Database services, network load balancing, in addition to IDS/IPS services. During vulnerability scanning and Proof of concept application analysis it was noted that CloudFlare was blocking and recording specific attempts at commonly known vulnerabilities. Including but not limited to SQL injection.

Voter privacy is ensured by removing client side storage of marked selections in browser history, allowing the voter to verify and save a ballot package for printing for use in a currently setup jurisdiction Absentee/ Mail-in voting program.

The ability to tamper with the client side application is always present due to the fact there are no server side verifications or validations in place after the ballot has been generated. In this context, however, the ability to affect large numbers of ballots is reliant upon server side compromise (initial DS ICR 5.2 RAVBM system ballot launch) which may also include; DDoS attacks, and the failure of the absentee/mail-in ballot system. The voter is given the ability to proof and confirm ballot selections within the DS ICR 5.2 RAVBM system interactive ballot system as well as the printed paper ballot.

Review of documentation showed that the TDP did not cover requirements 7.4.5 – Software Reference Information, or 7.4.6 Software Setup Validation.

Functional testing showed that requirements 7.4.5 – Software Reference Information, or 7.4.6 – Software Setup Validation, were not able to be verified to ensure that the system is running the correct software.

Potential vulnerability findings included potential issues for requirements 7.2.1. – General Access Control, where password autocomplete is enabled, 7.4.5 – Software Reference Information, where these is no verification method to ensure the correct applications are being run, and 7.8 Testing – Security, where potential cross site scripting, cross site request forgery, open redirection, SQL injection, untrusted SSL certificate, and strict transport security are not being enforced.

As per the direction given by the California Secretary of State, this security testing report does not include any recommendation as to whether or not the system should be approved.

End of RAVBMS Security and Telecommunications Test Report