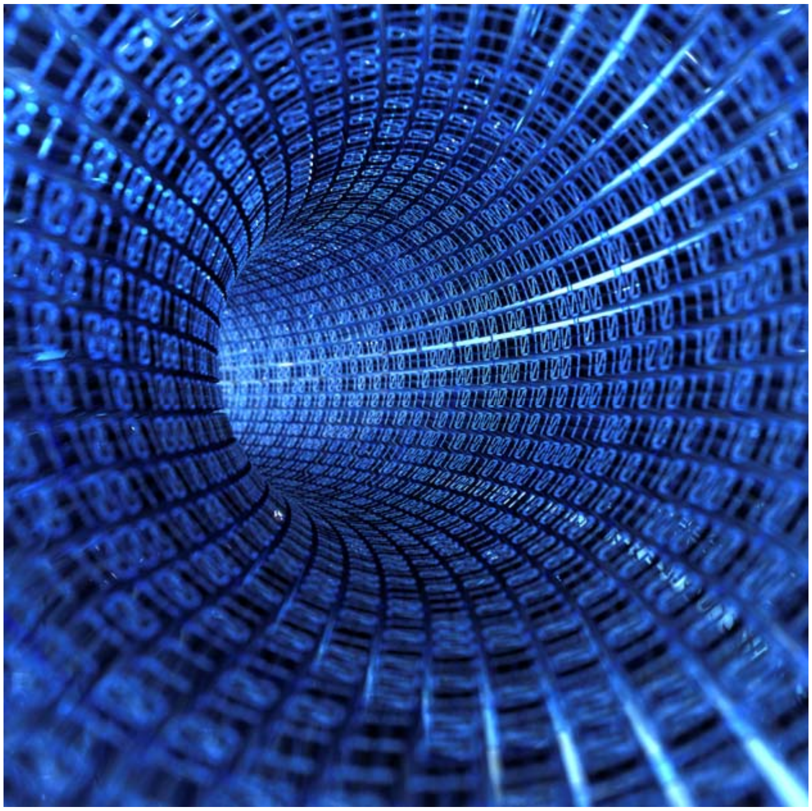

HART SYSTEM
MICROSOLVED, INC.
TECHNICAL DETAILS REPORT

CONFIDENTIAL[1]

[1] This report is released by Ohio Secretary of State Jennifer Brunner consistent with the Ohio Public Records Act, Ohio R.C. 149.43. The reader of this document is advised that any conduct intended to interfere with any election, including tampering with, defacing, impairing the use of, destroying, or otherwise changing a ballot, voting machine, marking device, or piece of tabulating equipment, is inconsistent with Ohio law and may result in a felony conviction under, among other sections, Ohio R.C. 3599.24 and 3599.27.

Table of Contents

Table of Contents

Overview

This report details the technical vulnerability findings of the MicroSolved, Inc. (MSI) penetration testing team. Our team was engaged by the Ohio Secretary of State to review the electronic voting systems used in Ohio as a part of the larger EVEREST project. Our testing took place from October 5th, 2007 through October 25th, 2007. As a part of our testing, significant security issues were identified in the Hart system at both a holistic level as well as at the lower level of many of the system components.

Purpose of this Report

This report is intended to be a catalog of the identified vulnerabilities within the Hart system and its components. Overall security implications and details of the engagement are contained in additional reports delivered to the Secretary of State's office.

The primary audience for this report is the technical staff or product management staff tasked with the mitigation of the identified security issues. Every effort has been made to make the findings of this report clear and the mitigation suggestions real-world based. Should additional information be desired, please do not hesitate to contact us through the Secretary's office for further discussions as appropriate.

Format of this Report

Each vulnerability will be discussed in reference to the impacted component of the overall Hart system. Each component has a specific section dedicated to it, with issues that impact several components in the final section named "General Multiple Component Vulnerabilities".

For each identified security issue, the following information is given:

Reference ID - Simply a unique reference to the specific issue. This is included to allow the readers a point of reference without complicated name issues.

Summary of the Vulnerability - A brief summary of the issue identified is included to give the reader the specific information needed to understand and locate the vulnerability.

Risk Rating - High, Medium or Low - We sorted the vulnerabilities at these levels to simplify their understanding and ease of association. High risk vulnerabilities are vulnerabilities that lead to the ability to modify the component's configuration, execute arbitrary code, modify election data or settings and/or introduce malware to the system. Medium risk vulnerabilities allow the attacker to gain additional information or examine the system in a way that could lead to further compromise. Low risk vulnerabilities are issues that impact the general performance or operation of the system, but yield little specific return when executed alone.

Impacted Pillar(s) - Confidentiality, Integrity, Availability - These three categories are often referred to as the pillars of information security. Security mechanisms must be created to prevent attacks that impact any of these three facets or reduce the impact of attacks against these categories to manageable levels.

Attack Prerequisites - What things must the attacker possess to exploit the vulnerability. Common prerequisites are things like specific knowledge, specific components or tools and access to specific parts of the system.

Attack Scenario - This section explains how or what an attacker might do to leverage the vulnerability and what the potential impact is of successful exploitation.

Mitigation Suggestion - This section explains what specific mitigation strategies or tasks are suggested for minimizing the risk or mitigating the issue.

A Warning About Cascading Failures

It should be noted that the risk rating identifies the potential risk of the vulnerability in isolation. However, attackers often use a process called "vulnerability chaining" to leverage multiple vulnerabilities in a system for further access or damage. Such a system of cascading failures obviously can change the impact and risk of specific vulnerabilities as they are combined and leveraged in new ways. Too many combinations and variables impact this situation to allow for comprehensive risk rating of each vulnerability in a cascade. Thus the risk and impact of specific issues may vary, depending on the attacker expertise, access and the presence of other vulnerabilities on the system that could be included.

System Components Included in this Report

This report includes vulnerabilities identified in the following Hart system components: eSlate DRE unit with PCMCIA memory card and VVPAT printer module, eScan optical scanner with PCMCIA memory card, CF memory card, plastic ballot box and paper ballots, Judges Booth Controller (JBC) Unit with PCMCIA memory card, Windows 2000 desktop computer, Windows 2000 laptop computer and the Hart elections management software package (BOSS/Tally/Rally/Servo/Trans/Ballot Now/eCM Manager/eCM). The final section (General Multiple Component Vulnerabilities) is reserved for vulnerabilities that were present on several of the components across the system.

DRE Component Vulnerabilities

ID #	DRE - 1
Vulnerability Summary	Movement of the DRE during the printing of barcodes causes multiple copies of the bar code to print on the VVPAT.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the component when it is printing barcodes, which is usual during voting.
Attack Scenario	Attackers could cause multiple barcodes to be printed, which if bar code recounts were used, could cause multiple vote counts for the same ballot. Note that bar code scanning of the VVPAT is presently not performed in Ohio. However, these odd barcodes could also confuse elections workers and cause chaos in the elections process.

Mitigation Suggestion(s)	The component should abort the vote if the bar code print is interrupted and should require a poll worker or command from the JBC to return to voting. If the bar code does not print in its entirety, then the bar code should be printed once and once only in the presence of the poll worker or the like. Awareness training should also be implemented to ensure that election workers are aware of the problem, how to handle misprints on the printed paper tapes and signs to look for in the polling place that could indicate attempts to tamper with the DRE.

Optical Scanner Vulnerabilities

ID #	OS - 1
Vulnerability Summary	Printed ballot serial numbers are predictable, not random.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to two or more ballots
Attack Scenario	Attackers could create their own ballots and deliver them via either absentee voting or at the precinct. This could be exploited to vote more than once per election.
Mitigation Suggestion(s)	Ballot sequence numbers should be randomly generated, not derived in a mathematical function.
ID #	OS - 2
Vulnerability Summary	Optical scanner ballot box locks can be trivially picked using common lockpicking techniques.
Risk Rating	High
Impacted Pillars	Integrity, Availability

Attack Prerequisites	Access to the ballot box
Attack Scenario	Attackers could open the ballot box and add or remove ballots. This could impact the integrity of the elections process.
Mitigation Suggestion(s)	Locks should be hardened against physical attack. Locks of higher quality with picking resistance should be implemented. Tamper tape could also be used to cover the locks to prevent arbitrary access without notice.
ID #	OS - 3
Vulnerability Summary	Operating system is loaded from an internal compact flash memory card that is protected solely by tamper tape.
Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the internals of the component
Attack Scenario	Attackers could simply replace the existing operating system with their own modified/tampered version that could be engineered to do anything from perform denial of service to change vote total operations. Detection is unlikely, as the OS could again be swapped post election or otherwise appear to be the original.
Mitigation Suggestion(s)	Security screws should be utilized on the case of the component to prevent casual opening. As mentioned elsewhere, implementation of case tamper detection switches would minimize the risk of this issue.
ID #	OS - 4
Vulnerability Summary	A second internal compact flash memory card slot is available and active inside the component.
Risk Rating	Medium
Impacted Pillars	Integrity, Availability

Attack Prerequisites	Access to the internals of the component
Attack Scenario	Attackers could leverage this second slot to insert their own compact flash card, possibly containing malware or other tampered code. This could result in complete compromise of the component, including election data. It is likely this attack vector would go undetected in all but the most severe of circumstances. If an attacker could later remove their memory card, it would be nearly impossible to determine its presence during an election.
Mitigation Suggestion(s)	The second compact flash slot should be removed or physically disabled.
ID #	OS - 5
Vulnerability Summary	The device is running a telnet server and the network port is fully exposed, even during elections. The team was unable to compromise the login and password used for access control on this service during the testing, however, large amounts of traffic to the service did appear to impact system performance.
Risk Rating	Low
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the device, a handheld or other computer and cable to complete the network connection
Attack Scenario	Attackers could use the easy availability to the network port to probe this telnet server for username/password combinations. Once a set of credentials are identified, the device could be fully compromised by the attacker. It is likely that malware could be introduced to the component in this manner and/or that elections data could be impacted, based upon the functionality that appears to be useable through the telnet interface when the binary image from the CF card was analyzed.
Mitigation Suggestion(s)	The telnet service should be disabled. The network port should be physically disabled just as the other ports on the device are - or at a minimum the network port should be covered with tamper tape to prevent access during the elections cycle.

Judges Booth Controller (JBC) Vulnerabilities

ID #	JBC - 1
Vulnerability Summary	Voter access codes are predictable.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to a number of codes in the order in which they were generated (this number is likely to be less than 25 codes in sequence)
Attack Scenario	Attackers could leverage this vulnerability to attack the voting process. They could predict access codes and based upon line length, vote multiple times - thus gaining more than normal voter influence and destroying the integrity of the elections process.
Mitigation Suggestion(s)	Voter codes should be randomly generated by the JBC to prevent prediction. Each code should be generated rather than mathematically derived.

Windows 2000 Desktop Computer Vulnerabilities

ID #	DSK - 1
Vulnerability Summary	Component lacks best-practice security mechanisms such as a firewall, anti-virus software and Digital Guardian.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the component at any time during its lifetime

Attack Scenario	Attackers could leverage this lack of controls to further their goals of introducing malware into the components. If access to the components is gained either physically, logically or over the network - then attackers could cause complete compromise.
Mitigation Suggestion(s)	Components should be deployed with firewalls and anti-virus applications in place. Processes should be created to ensure that these applications are kept up to date without exposing the components to the Internet or other untrusted networks. Digital Guardian should be deployed on this component to enforce the white list of applications that can be executed on the component. Digital Guardian should also enforce other rules and controls as desired by the SoS to ensure the integrity of the component and its data.
ID #	DSK - 2
Vulnerability Summary	Component is not configured in accordance with industry standard best practices. Examples: Password policies are not properly configured. Logging is not properly configured. Windows is not configured with adequate security settings. Windows is missing critical hotfixes/patches.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the component/network
Attack Scenario	Attackers who gain access to the component/network or malicious users can easily compromise the system, install malware or perform other illicit operations.
Mitigation Suggestion(s)	The systems should be deployed in accordance with industry standard best practices as defined by NIST, SANS, the Center for Internet Security, etc. Adoption of these standards and changes to the configuration to become compliant with their requirements would greatly enhance the security posture of the system.

ID #	DSK - 3
Vulnerability Summary	A default account called "[redacted]" with a default password of "[redacted]" exists on the system as an administrator. This account was able to be enumerated remotely. The password was trivially cracked using common tools from the Internet.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Knowledge of the default credentials or access to the component
Attack Scenario	Attackers who gain physical or network access to the component could use this default account to completely compromise the component, introduce malware to the component and/or modify elections data.
Mitigation Suggestion(s)	All default accounts should be removed from all components.

Windows 2000 Laptop Vulnerabilities

ID #	LTP - 1
Vulnerability Summary	Component lacks best-practice security mechanisms such as a firewall, anti-virus software and Digital Guardian.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the component at any time during its lifetime

Attack Scenario	Attackers could leverage this lack of controls to further their goals of introducing malware into the components. If access to the components is gained either physically, logically or over the network - then attackers could cause complete compromise.
Mitigation Suggestion(s)	Components should be deployed with firewalls and anti-virus applications in place. Processes should be created to ensure that these applications are kept up to date without exposing the components to the Internet or other untrusted networks. Digital Guardian should be deployed on this component to enforce the white list of applications that can be executed on the component. Digital Guardian should also enforce other rules and controls as desired by the SoS to ensure the integrity of the component and its data.
ID #	LTP - 2
Vulnerability Summary	Component is not configured in accordance with industry standard best practices. Examples: Password policies are not properly configured. Logging is not properly configured. Windows is not configured with adequate security settings. Windows is missing critical hotfixes/patches.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the component/network
Attack Scenario	Attackers who gain access to the component/network or malicious users can easily compromise the system, install malware or perform other illicit operations.
Mitigation Suggestion(s)	The systems should be deployed in accordance with industry standard best practices as defined by NIST, SANS, the Center for Internet Security, etc. Adoption of these standards and changes to the configuration to become compliant with their requirements would greatly enhance the security posture of the system.

ID #	LTP - 3
Vulnerability Summary	A default account called '[redacted]" with a default password of '[redacted]" exists on the system as an administrator. This account was able to be enumerated remotely. The password was trivially cracked using common tools from the Internet.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Knowledge of the default credentials or access to the component
Attack Scenario	Attackers who gain physical or network access to the component could use this default account to completely compromise the component, introduce malware to the component and/or modify elections data.
Mitigation Suggestion(s)	All default accounts should be removed from all components.

Hart Elections Management Software Vulnerabilities

ID #	SW - 1
Vulnerability Summary	Manual editing of election data is possible using a feature built into Tally. This allows election vote totals to be modified directly without additional authentication, though the event is logged in the database.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the Tally software, including a elections worker login and password

Attack Scenario	Attackers could leverage this vulnerability manually or through malware introduced to the system to change the vote totals. It is likely that such changes would go unnoticed and/or that the appropriate log entries could be removed from the database.
Mitigation Suggestion(s)	Manual editing of the elections data should be removed from the main function of the application and introduced in a manner that only allows access through multi-factor authentication or other method. In addition, any reports or other output of the results or other relevant data to the election should include a notification that the data has been edited/altered. If possible, manual election data editing should be removed entirely to minimize this threat.
ID #	SW - 2
Vulnerability Summary	Rally to Tally communications are not fully encrypted. The protocol in use transfers some data in plain text. SSL is not implemented in accordance with best practices.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the network
Attack Scenario	Attackers could capture and or modify the data in transit, thus impacting the integrity of the election.
Mitigation Suggestion(s)	All connections between components should be fully encrypted using an industry standard peer reviewed cryptographic algorithm such as SSL.
ID #	SW - 3
Vulnerability Summary	Databases containing elections data are not encrypted.
Risk Rating	High
Impacted Pillars	Integrity

Attack Prerequisites	Access to the component/file system
Attack Scenario	Attackers could edit or change the contents of the database or deploy malware that would edit or change the contents of the database at any time. Given the lack of the malware defenses on the PC systems, such an attack would likely be effective and unnoticed.
Mitigation Suggestion(s)	Databases containing elections data and critical configuration information about the system should be fully encrypted using an industry standard encryption mechanism. The deployment of Digital Guardian, if properly configured, as suggested in the previous sections of this report would also help to minimize the risks stemming from this issue.
ID #	SW - 4
Vulnerability Summary	Sensitive data is exposed as plain text strings inside the software binaries. Items such as passwords, SQL statements and other sensitive items were easily identified using basic tools such as notepad.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the binaries
Attack Scenario	Attackers could analyze the binaries to discover critical information about the system. This could allow them to easily map the database tables, identify login and password information and other items that could be leveraged to compromise the component or system and the core elections data.

Mitigation Suggestion(s)	Sensitive information should not be stored as plain text strings in binaries. Other areas such as encrypted files or protected registry entries should be used instead. If information must be embedded in a binary, best practices dictate that it be obfuscated in some manner. The vendor should adopt a baseline of best practices for secure software development and educate their development staff on the guidelines. Their quality process should also be adjusted to ensure that these guidelines are being followed in all of their applications. Applicable guidance for these activities is publicly available from NIST.

General Multiple Component Vulnerabilities

ID #	GMC - 1
Vulnerability Summary	Many components (Rally, Tally, JBC, Optical Scanner) fail to recognize copied and tampered vote data. The components do not alert upon identifying tampered data in many cases, they simply ignore the specific data in question.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the memory cards
Attack Scenario	Attackers could use this lack of detective controls to systematically probe the system for vulnerabilities and ways to change vote totals over time with little to no chance of detection. Votes could also be tampered to ensure that they are not counted and such tampering would likely go undetected as the system does not alert upon noticing tampered vote data.
Mitigation Suggestion(s)	When vote data appears on the card that is invalid, the system should log and alert as appropriate. In addition to ignoring the illicit vote data (which it does), it should alert the system administrators that tampered data may be present on the memory cards. The addition of a checksum mechanism to the various components would likely assist in detecting illicit data on the cards.

ID #	GMC - 2
Vulnerability Summary	PCMCIA memory cards used to store and transport vote totals from optical scanners and the JBC do not encrypt the voting data. Our team was able to easily read and edit the contents of the memory card using a drive available for purchase over the Internet and the included software. It should be noted that this did NOT require access to the eCM key to perform, as it was done outside of the Hart software.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the memory cards
Attack Scenario	This vulnerability opens a plethora of attack scenarios. Because the memory cards are not encrypted attackers can alter the contents of the voted ballots, arbitrarily tamper with the elections data and even retrieve the voting data for correlation with voter sign-ins and other records that break the veil of secrecy around the voter's specific vote in some circumstances.
Mitigation Suggestion(s)	Voting data stored on all media should be encrypted to prevent tampering. While additional procedural controls should be implemented to enhance attention to custody of and access to the memory cards, strong encryption is the best practice solution for minimizing the risks associated with this issue. The vendor should immediately implement encryption of all
ID #	GMC - 3
Vulnerability Summary	None of the components include electronic sensors to detect if their cases have been opened or tampered with.
Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the components

Attack Scenario	Attackers could utilize the lack of case sensors to probe the internals of the hardware, introduce Trojan hardware/firmware/software and perform other kinds of attacks.
Mitigation Suggestion(s)	Case sensors should be introduced on all components. Sensors that alert the operator of case tampering are common on PC systems and should be implemented on future versions of the hardware. Tamper seals are in place today, but could be easily circumvented.
ID #	GMC - 4
Vulnerability Summary	Passwords for election management functions on many devices (DRE, optical scanner, JBC) are numeric only and a maximum of six digits.
Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the components
Attack Scenario	Attackers could easily guess these passwords or observe them, allowing access to elections management functions.
Mitigation Suggestion(s)	Passwords should be implemented on all components in accordance with industry standard best practices. This should include alpha-numeric characters and minimum password lengths of eight or more characters. In addition, mechanisms to log and alert on attempts to brute force the passwords should be implemented.

Summary

This report is intended to be a catalog of the identified vulnerabilities within the Hart system and its components. Overall security implications and details of the engagement are contained in additional reports delivered to the Secretary of State's office.

Significant issues were identified during our review. Most of these issues seem to stem from a lack of adoption of industry standard best practices. Configuration changes, modification of default implementations and significant changes to the application and system architectures are required to mitigate the identified issues. These mitigation suggestions should be implemented as soon as possible to minimize the opportunity for exploitation by attackers. Additional mitigations or minimization of risks is likely possible through policy and process changes. This is explored in additional report documents delivered to the Secretary of State.