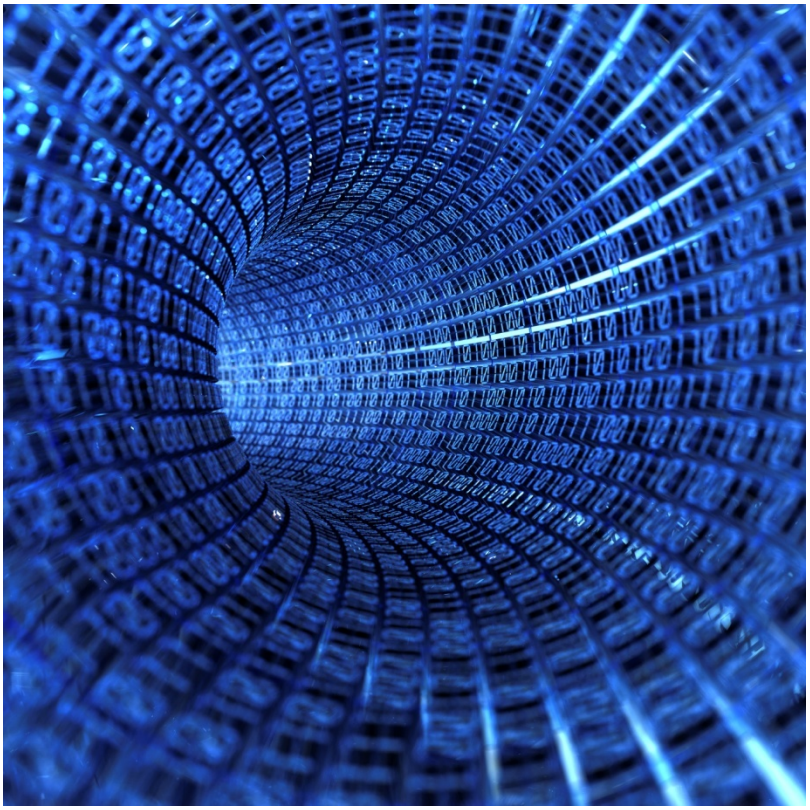

PREMIER SYSTEM

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 Premier 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 Premier 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 Premier 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 Pre-Requisites - 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 to 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 Premier system components: DRE System, Central Optical Scanner and Precinct Optical Scanner (the same hardware with different firmware and deployment scenarios), Digi PortServer II Device, Electronic Poll Worker (EPW) System, Elections Media Processor (EMP) Workstation and Election Media Processor (EMP) Software, GEMS Server, and the GEMS Software (includes the smartcard software component). Other components of the system were tested, but either had no identified issues or are simply subsystems whose issues are included in their larger components. For example, the actual paper ballots were tested as a part of optical scanner testing and relevant findings are included in those sections. The memory card media was also tested, but the findings are included in the larger components where impact is likely to occur such as the DRE, EMP Server or GEMS Software.

DRE System Vulnerabilities

ID #	DRE - 1
Vulnerability Summary	Component problems during boot cause system to boot into administrative mode
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the system during boot, attacks on memory card slot requires PCMCIA card with zero byte files or directories to prevent file system operations, attacks on smartcard slot require credit card or smart card, attacks against the printer require it to simply be knocked from position such as from a sharp blow or intentional tampering

Attack Scenario	Attackers who can cause hardware issues to the printer, smartcard slot or file system of the memory card during the boot sequence could cause the system to enter administrative modes. From this mode, changes to the DRE settings, election details and elections data are possible. In some cases, replacing cryptographic keys or logs are also possible. Simply holding a smart card in the reader's deepest setting during boot causes boot to administrative mode. Other researchers also identified this issue using a paper clip to cause the error. Filling the memory card with enough zero byte files or directories also causes the DRE to boot into administrative mode if the file system can not create the proper files for system operation.
Mitigation Suggestion(s)	Trim down boot error condition modes to allow access to only the specific requirements needed to troubleshoot or repair the problem. For example: If the printer is in error, the system should enter a mode where the only administrative function available is related to troubleshooting or repairing the printer. In the event of a smartcard reader issue, the system should only allow access to the smartcard reader reset and test functions. Memory card file system problems should display messages to replace the card with a proper one and allow reboot. General administrative access when a failure condition occurs during boot is too powerful for the deployment scenarios these systems face.
ID #	DRE - 2
Vulnerability Summary	Buffer overflows exist in the DRE application that can be exploited by manipulating the "[redacted]" file on the memory card.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the memory card, ability to deliver malicious PCMCIA card

Attack Scenario	Attackers could exploit this vulnerability by placing a malicious PCMCIA card into the memory card slot. The "[redacted]" file is loaded by the system as it accesses the election files needed to operate. Attackers leveraging these buffer overflows could likely execute arbitrary code on the system and/or affect system availability. This technique is likely an attack vector for the planting of malware on the DRE system, which other research has proven possible - including replication back to the GEMS Software and Server.
Mitigation Suggestion(s)	All applications on the DRE should undergo source code analysis and any identified weaknesses in input validation techniques should be repaired. All inputs on all DRE applications should perform proper bounds checking to prevent buffer overflows.
ID #	DRE - 3
Vulnerability Summary	Known file names and extensions can be used to load arbitrary code onto the DRE - namely "[redacted]", "[redacted]" and "[redacted]"
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the memory card slot during boot, malicious PCMCIA card, knowledge of file formats specific to the system
Attack Scenario	Attackers could leverage this data that is publicly available on the Internet to compromise DRE systems. Exploiting this vulnerability could allow them to overwrite any file on the system or execute arbitrary code with little chance of detection. The files do not appear to be checked for authentication of any kind prior to loading.
Mitigation Suggestion(s)	There are many options for mitigating this issue. Code signing mechanisms could be employed to prevent arbitrary code inclusion if implemented properly. The feature could be disabled unless a specific internal jumper or smartcard were present or the mechanism could be removed entirely if in-the-field updates are not required.
ID #	DRE - 4

Vulnerability Summary	Physical security of the DRE case is inadequate to prevent casual tampering and disassembly
Risk Rating	Medium
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the DRE system outside of the polling place or without supervision, screwdriver, malicious electronics or software systems
Attack Scenario	Attackers could easily disassemble the DRE system without any special tools. No electronic sensors identify that any tampering has taken place. Once the case is removed, the addition of malicious hardware, tampering with internal components or software/firmware are likely possible, as are access to internal debug and diagnostic functions. Attackers could likely leverage this access to implement malware, malicious hardware or other changes to the system that could impact the confidentiality, integrity or availability of the DRE system during an election.
Mitigation Suggestion(s)	Premier should replace the case screws with special security screws to make the disassembly more difficult and time consuming, as well as requiring special tools. The inclusion of an electronic sensor to alert users to the opening of the case is also a common solution and is implemented in many PCs and other devices today. Physical tampering could also trigger audio alerts to further safeguard the internal components.
ID #	DRE - 5
Vulnerability Summary	The DRE system lacks any meaningful mechanism for intrusion detection and cyber tampering logging/alerting.
Risk Rating	Medium
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the network, file system or memory card subsystems

Attack Scenario	Attackers could leverage the lack of detection mechanisms on the DRE systems to systematically probe the file system, memory card system and/or network presence for weaknesses. Tampering with the memory card contents, the network traffic or other parts of the DRE system did not alert the users or administrators in any meaningful and effective way. The minimal coverage of the audit logs contained on the DRE system and the memory cards are not sufficient to protect the DRE from compromise and attack.
Mitigation Suggestion(s)	Premier should implement intrusion detection capabilities on the DRE. Logging and audio/visual alerting should be implemented whenever an error condition, anomalous event or other actions that could indicate tampering occur. Standard processes for auditing the systems against possible signs of electronic tampering should then be implemented by all Boards of Election.
ID #	DRE - 6
Vulnerability Summary	Physical security of the primary memory slot cover is inadequate to properly protect the power button, memory card and memory card ejection button, even with tamper seals applied.
Risk Rating	Low
Impacted Pillars	Availability
Attack Prerequisites	Access to the system, small thin firm implement (pocket knife blade, lockpick, etc.)
Attack Scenario	Attackers could exploit this vulnerability to cause availability issues in the field or to reboot the system. The attacker simply slips the tool between the protective cover and the body of the DRE and is able to power the system on/off and eject the memory card from the system (though not replace it with another without picking the lock, breaking the case and/or the seal). Likely, this could be used to cause a poll worker to reboot the system in front of the user and potentially expose the memory card slot to manipulation in certain social engineering scenarios. Given the seriousness of the security issues surrounding the DRE boot process detailed above, this attack could likely be chained with others to compromise a DRE.

Mitigation Suggestion(s)	The cover for the memory slot bay should be changed to snap into place physically and then lock. The could even include interior edging to protect against the insertion of tools into the space between the cover and the body of the DRE. The tamper tape seals can be deployed horizontally across the top of the cover and the DRE while the door is held tightly in place with the other hand. Such placement of the tamper seals makes the vulnerability harder (though not impossible) to exploit without detection. A standard for the placement of all tamper seals and their orientation should be created and adopted by all Boards of Election.
ID #	DRE - 7
Vulnerability Summary	Physical security of the printer unit is not sufficient to protect it against displacement or tampering that could result in an operation error and trigger the need to reboot the DRE system.
Risk Rating	Low
Impacted Pillars	Availability
Attack Prerequisites	Physical access to the DRE, such as in a polling location
Attack Scenario	An attacker could simply deliver a sharp blow or a large amount of leverage to the printer unit (such as by a feigned fall or the like). If sufficient to dislodge it from its normal state, the DRE system will not function and reboot by a poll worker is likely. Again, given the DRE boot issues detailed above, social engineering scenarios chaining this issue with others could possibly result in illicit access to the DRE subsystems and/or the compromise of the DRE.
Mitigation Suggestion(s)	Structural improvements should be implemented to keep the printer in position and operation and to make physical tampering more difficult. The case itself should be made more secure against attempts to dislodge the printer.

Central and Precinct Optical Scanner Vulnerabilities

In our testing, these devices were found to exhibit the same issues. Note that they are the same hardware platform with different configurations, firmware and deployment scenarios.

ID #	OS - 1
Vulnerability Summary	Paper ballots are not serialized and can be scanned multiple times.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the central scanner and/or to the ballots themselves, failure of general auditing processes
Attack Scenario	Because the ballots themselves are not serialized and no system detection of duplicate ballots takes place it is possible for duplicate ballots to be scanned by the system. Currently, Boards of Election audit the ballot counts and perform some level of inspections and dual-access controls to overcome these issues, but inclusion of electronic mechanisms would make this work less resource intensive and more accurate.
Mitigation Suggestion(s)	Optical scanning and paper ballot systems should become serialized to prevent tampering and rescan of ballots without notification. Proper memory and management systems should be implemented into the system to allow for this.
ID #	OS - 2
Vulnerability Summary	Modifications of the paper ballot are difficult to detect and could be used to disrupt the elections processes.
Risk Rating	Low
Impacted Pillars	Availability
Attack Prerequisites	Access to ballot stock or similar paper, a way to introduce the malicious ballots into the process (possibly via mail or the like for absentee ballots)

Attack Scenario	Attackers could modify paper ballots or create their own paper ballots to resemble the election ending control ballots, diagnostic ballots or the like. Such an attack would be easily detected once performed, but the manual detection of such changes to the ballots is difficult by human eye. Attackers exploiting this scenario are unlikely to influence elections in a meaningful way, but could cause delays, frustrations and general chaos.
Mitigation Suggestion(s)	Other means of performing diagnostic mode changes and election start/stop could be implemented that did not rely on the optical mechanism. This would likely mitigate the possibility of exploiting this type of attack from the public. Serialization of the ballots would also reduce the capability to perform this attack.

Digi PortServer II Vulnerabilities

ID #	DPS - 1
Vulnerability Summary	Poor password controls in place on the device
Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the network or system interfaces
Attack Scenario	Attackers with access to the network or system interfaces of the device could modify its configuration and operation. Accounts without passwords and with easily guessed passwords are present on the system (such as accuvote and root/global). Changes to the operation of the system could be made that could impact the general availability of the Central Optical Scanner and could make troubleshooting time consuming and difficult. Common password brute force tools were quickly successful in obtaining administrative access to the system.

Mitigation Suggestion(s)	Strong passwords need to be implemented on all components across the Premier systems. A proper password policy should be identified and adopted by all Boards of Elections.
ID #	DPS - 2
Vulnerability Summary	The device offers unneeded network services, thus increasing its risk posture.
Risk Rating	Low
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the network interface of the device
Attack Scenario	Attackers could identify vulnerabilities in these services and use them to exploit the device and obtain access to it. Attackers could also exploit these services to cause denial of service conditions on the device and tamper with the availability of the central optical scanning system that requires this device to operate.
Mitigation Suggestion(s)	Unneeded services should be removed from operation.

Electronic Poll Worker Vulnerabilities

ID #	EPW - 1
Vulnerability Summary	Buffer overflows exist in the edit fields of the main application.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the system, a USB keyboard

Attack Scenario	An attacker can input long streams of input into the edit fields on the main screen of the application before the poll data file is loaded. By inputting long strings of characters into these fields a buffer overflow appears to be triggered causing the system to crash and potentially exposing the system to arbitrary code execution.
Mitigation Suggestion(s)	All edit fields in the application should be implemented in a read only fashion if they are not intended for user input. All applications on this system should undergo a source code review to identify possible vulnerabilities. All user input should perform proper bounds checking.
ID #	EPW - 2
Vulnerability Summary	Known file names offer the ability to install arbitrary code on the system using the memory card slots - specifically "[redacted]".
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the memory card slots during boot, malicious memory card, knowledge of file formats specific to the system
Attack Scenario	Attackers could leverage this data that is publicly available on the Internet to compromise DRE systems. Exploiting this vulnerability could allow them to overwrite any file on the system or execute arbitrary code with little chance of detection. The files do not appear to be checked for authentication of any kind prior to loading.
Mitigation Suggestion(s)	There are many options for mitigating this issue. Code signing mechanisms could be employed to prevent arbitrary code inclusion if implemented properly. The feature could be disabled unless a specific internal jumper or smartcard were present or the mechanism could be removed entirely if in-the-field updates are not required.
ID #	EPW - 3
Vulnerability Summary	The device is running a web server which is not required for its functionality.

Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the network interface
Attack Scenario	Attackers could identify previously unknown vulnerabilities in this web server (none are currently known) and use it to compromise the system or cause denial of service conditions.
Mitigation Suggestion(s)	Disable the web server on the default configuration of the device.

Election Media Processor (EMP) Workstation Vulnerabilities

ID #	EMPW -1
Vulnerability Summary	Some mutated ballot files could be uploaded via the EMP that would cause the precinct to be shown as reported but the votes would not be added to the tally. The mutation must be slight enough to allow the EMP system to believe it is valid but for GEMS to be unable to properly decrypt the file. Neither the EMP software nor GEMS alerts or logs the problem and we identified no mechanism for determining if this attack had taken place other than raw auditing of the vote tapes against the tally system. Proper mutation of the ballot file was successful in several cases where the mutations were more than 4096 bytes into the ballot file and primarily when null bytes (hex 00) were mutated to hex AA. Other mutation sets with predictable outcomes were not identified, though the vulnerability showed itself frequently during the testing with seemingly random inputs and results.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the memory card, knowledge of the proper mutation, failure of audit systems

Attack Scenario	An attacker leveraging this exploit could mutate the election files from specific precincts and systems with the intent of altering the outcome of the election. Doing so in a busy election would likely go unnoticed unless an audit were performed against the paper tapes. Note that this may also be possible with a corrupted ballot file that occurs due to system error. We were unable to identify a specific case, but could likely happen if failures occurred with the memory card, read or write devices or file systems.
Mitigation Suggestion(s)	The EMP system should implement the same validation techniques that the DRE uses to inspect and validate the ballot file. This should be done by the EMP system before it passes the data to GEMS. Improper ballot files should cause alerts about possible tampering. GEMS should alert and log the fact that decryption errors occur with the ballot files. This should be cause for investigation and handled as a possible attempt to tamper with the system.
ID #	EMPW - 2
Vulnerability Summary	EMP workstation system is not configured in accordance with industry standard best practices. Examples: BIOS passwords are not enabled. Password policies are not properly configured. Logging is not properly configured. Windows is not configured with adequate security settings.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Physical access to the system
Attack Scenario	Attackers who gain physical access to the system 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 or the Center for Internet Security. 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 #	EMPW - 3
Vulnerability Summary	The EMP system does not have a firewall or anti-virus software in place.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the system
Attack Scenario	Attackers could leverage these weaknesses to obtain illicit access to the system, escalate their privileges and/or install malware. The lack of common defensive tools on this component of the Premier system does not match the defensive mechanisms in place on the GEMS server.
Mitigation Suggestion(s)	Premier should adopt and deploy a common set of up to date tools for protecting the EMP workstation and other components. At the very least a basic anti-virus package should be installed and used along with the Windows firewall. Boards of elections should adopt procedures for ensuring that these defensive tools and the operating system of the EMP workstation stay up to date. They should identify mechanisms for doing this that DOES NOT INCLUDE exposing these systems to the Internet or any other populated network.

Election Media Processor (EMP) Software Vulnerabilities

ID #	EMPS - 1
Vulnerability Summary	The EMP software is vulnerable to buffer overflows in the "[redacted]" file from the memory card. Exploitation of this buffer overflow leaves the attacker in control of the processor's EIP, allowing for the execution of arbitrary code.

Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the memory card, ability to deliver malicious memory cards
Attack Scenario	Attackers could exploit this vulnerability by delivering a malicious memory card for processing. The "[redacted]" file is loaded by the system as it accesses the election files needed to operate. Attackers leveraging these buffer overflows could likely execute arbitrary code on the system and/or affect system availability. This technique is likely an attack vector for the planting of malware on the EMP system.
Mitigation Suggestion(s)	All source code within the EMP application should undergo review for possible security issues. All application inputs should perform proper bounds checking.

GEMS Server Vulnerabilities

ID #	GS - 1
Vulnerability Summary	GEMS server system is not configured in accordance with industry standard best practices. Examples: Passwords are easily guessable. Autorun is enabled. Password policies are not properly configured. Logging is not properly configured. Windows is not configured with adequate security settings.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability

Attack Prerequisites	Physical access to the system
Attack Scenario	Attackers who gain physical access to the system 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 or the Center for Internet Security. 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 #	GS -2
Vulnerability Summary	Digital Guardian software is not configured properly. This is a critical piece of protecting the election data and the GEMS server from known vulnerabilities identified in other reports and tests. However, the software is not configured to block many of the actions it claims to block. It simply alerts the user that the action is being logged and blocked, but allows the actions to be performed anyway. Further, the software is not configured to create logs, thus rendering it incapable of providing audit capability for intrusion detection, tampering attempts or other illicit actions.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the system, network access if other issues are leveraged
Attack Scenario	Users of the system or attackers gaining access will find that few options are blocked by the present configuration of Digital Guardian. Workarounds exist for most, if not all, operations currently restricted by the tool. As configured, it is providing little to no additional protection for the system or the data.

Mitigation Suggestion(s)	Configuration changes to Digital Guardian are needed. Enforcement mode should be enabled widely across the system and logging of any action outside of normal user behavior should be logged and alerted on. Ongoing refinement of the rule set of Digital Guardian will be required. The Secretary of State and the Board of Elections should establish common update mechanisms and processes.
ID #	GS - 3
Vulnerability Summary	Digital Guardian is easily disabled. Our team killed the program using a freely available tool from the Internet called "Ice Sword". Most utilities capable of detecting hidden processes and terminating them are likely to be effective ways to disable the protection of Digital Guardian. Programs written for the purpose of eliminating "root kits" seem to be quite effective at identifying and killing the Digital Guardian applications. Given the poor configuration of both Digital Guardian and the over all server operating system, no evidence of the attack was identified or logged. Since no icon or other visual indicator is shown by Digital Guardian, no detectable change in the interface would alert users to the lack of Digital Guardian protection.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the system, tool or malware to kill Digital Guardian
Attack Scenario	Attackers could either manually kill the applications or create custom software that could be delivered on CD, via USB device or over the network. Once Digital Guardian was disabled, the malicious code could perform attacks against GEMS or other components and even restore Digital Guardian to operation when it was completed. Likely, such an attack would go unnoticed unless someone actually observed the delivery mechanism being used. Given the insecure environments of many Boards of Election, this is likely to be possible during times when elections are not active.

Mitigation Suggestion(s)	Digital Guardian should be configured with an application white list. Only applications on the white list (which would be restricted to required applications for election management and processing) should be allowed to be executed. Any attempt to execute any other program, application or code should result in alerts and logging of the illicit activity.
ID #	GS - 4
Vulnerability Summary	Digital Guardian does not adequately protect the GEMS software and database from tampering. Digital Guardian protects against some activities based upon context of the account used to perform the actions. Rules and capabilities vary for the three enabled known users: Administrator, gemsadmin and gemsuser. However, operations or access performed in the SYSTEM context are not affected by Digital Guardian's protection. SYSTEM context is commonly the context gained by attackers using exploits or through manipulation of the scheduler/at service in Windows.
Risk Rating	High
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the system, method of gaining SYSTEM context
Attack Scenario	Attackers could leverage known accounts, current access if available or malware to gain the SYSTEM context. Once in SYSTEM mode, attacks against GEMS directly could be performed without the protection of Digital Guardian.
Mitigation Suggestion(s)	SYSTEM context should be added to the ruleset of Digital Guardian and should not be able to bypass the rules or white list of applications suggested elsewhere in this document.
ID #	GS - 5

Vulnerability Summary	The Windows 2000 Server initiates the TCP/IP services prior to enabling the Sygate firewall installed on the system. This allows for a few moments of connectivity to the system and exposes it to possible network compromise or malware infection.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the network interface during reboot
Attack Scenario	An attacker or malware could exploit password vulnerabilities or other weaknesses to gain access to the server system. Such a compromise could be accomplished by watching for the system to reboot or observance of network traffic to detect the reboot cycle.
Mitigation Suggestion(s)	Likely the solution to this issue is not going to be created for Windows 2000, given its end-of-life position. This issue does not exist in Windows XP or 2003. The server should be upgraded to a currently supported operating system as soon as practical.
ID #	GS - 6
Vulnerability Summary	The firewall and anti-virus software on the GEMS server can be terminated and modified by any user.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the system
Attack Scenario	Users of the system, or attackers gaining access, can terminate the firewall and/or virus protection for the system. The applications do not automatically restart when the user logs out or in unless the system is rebooted.

Mitigation Suggestion(s)	Only the Administrator should be able to alter the firewall or virus protection systems and/or terminate their operation. The applications should automatically restart at any login to the system. Alternatively, both applications could be configured to enforce their password requirements for changes and termination. If enabled with strong passwords and secrecy is maintained, this would mitigate this issue.
ID #	GS - 7
Vulnerability Summary	The firewall and anti-virus signatures are out of date. The anti-virus signatures on the GEMS server we inspected had not been updated since 2005.
Risk Rating	High
Impacted Pillars	Confidentiality, Integrity, Availability
Attack Prerequisites	Access to the system or network
Attack Scenario	Attackers could leverage these issues to perform network attacks or introduce malware into the system. Given that the signatures for detection are so far out of date, the efforts required to produce malware that will not be detected by the anti-virus application is significantly reduced. This effectively increases the field of potential attackers.
Mitigation Suggestion(s)	Premier should update the signatures used on their default images to be more current with attack detection. Boards of Election should adopt a method of updating the signatures of these products without exposure to the Internet or other populated networks. This should be done in a secure fashion with ongoing regularity.
ID #	GS - 8

Vulnerability Summary	The operating system of the GEMS server is out of date. General support for Windows 2000 has ended. No functionality or non-security updates will be released for this operating system. It is currently scheduled for end of life in 2015.
Risk Rating	Low
Impacted Pillars	Availability
Attack Prerequisites	None
Attack Scenario	None
Mitigation Suggestion(s)	The operating system should be upgraded to Windows 2003 Server or whatever certified platform Premier makes available. This should be done as soon as practical for all GEMS servers throughout Ohio.

GEMS Software Vulnerabilities

ID #	GEMS - 1
Vulnerability Summary	Votes database may be edited using common tools without detection by the GEMS software. GEMS lacks encryption and integrity verification capabilities for its files and databases.
Risk Rating	High
Impacted Pillars	Integrity
Attack Prerequisites	Access to the system, removal of protections provided by Digital Guardian

Attack Scenario	An attacker or malware could remove the protections of Digital Guardian and then directly edit the GEMS database using common applications capable of editing Access databases. Election information, vote counts and the like could be changed. GEMS, itself does not detect any illicit changes to the database file and does not appear to perform any integrity checking of the database contents.
Mitigation Suggestion(s)	Mitigation of this vulnerability is difficult without extreme changes to the GEMS application architecture. Common solutions to these issues include encrypting the database to resist editing directly, or the implementation of transaction-level authentication which evaluates the security of each and every record within the database application. Premier should add encryption and verification capabilities as described or through some other mechanism as soon as possible.
ID #	GEMS - 2
Vulnerability Summary	Fuzzing of GEMS files revealed exception handling problems within the GEMS application. By fuzzing applications and database files, it was possible to cause GEMS to crash with unhandled exceptions.
Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the system and the directory of GEMS files, removal of the Digital Guardian protections
Attack Scenario	Attackers could use these unhandled exceptions to potentially cause damage to database file integrity or to disable the GEMS application. Troubleshooting and repair could be difficult.
Mitigation Suggestion(s)	Better exception handling and error reporting should be implemented in the GEMS application. Exceptions should always report a cause or specific error message that can be used to locate and repair the issue. The source code of the GEMS applications should undergo an assessment for potential security or performance issues which could be leveraged by an attacker.

ID #	GEMS - 3
Vulnerability Summary	GEMS audit logs show only successful logins and does not record failed attempts to access the database.
Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the system and GEMS software
Attack Scenario	Attackers with access to the system could easily brute force the passwords of the databases within GEMS. Little chance of detection of such an attack exists due to the lack of logging of the attempts. Essentially this gives attackers and malware an open opportunity to brute force the passwords of the database.
Mitigation Suggestion(s)	Premier should implement additional logging in the GEMS application to show failed logins and any other potential signs of attempts to tamper with the application or its data.

General Multiple Component Vulnerabilities

ID #	GMC - 1
Vulnerability Summary	Physical locks on the various components are easily circumvented using common lockpicking techniques. Keys are common among components and commonly available over the Internet. Affected components include: optical scanners, DRE units and ballot sorting/storage units
Risk Rating	Medium
Impacted Pillars	Integrity, Availability
Attack Prerequisites	Access to the system, knowledge of lockpicking, tools
Attack Scenario	Attackers with physical access to the devices and components could steal ballots, tapes, memory cards and other items. They could also tamper with or destroy components causing delays or other availability issues.
Mitigation Suggestion(s)	The locks need to be upgraded to more secure hardware. Keys should be system/device specific and access to the key sets should be controlled by strong processes. Where possible, tamper seals should be utilized in a common fashion to minimize the risks from this threat.

Summary

This report is intended to be a catalog of the identified vulnerabilities within the Premier 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.