# VIRGINIA INFORMATION TECHNOLOGIES AGENCY

# COMMONWEALTH SECURITY AND RISK MANAGEMENT

---

# SECURITY ASSESSMENT OF WINVOTE VOTING EQUIPMENT FOR DEPARTMENT OF ELECTIONS

---

APRIL 14TH, 2015

## Executive Summary

During a recent election, one precinct in Virginia reported unusual activity with some of the devices used to capture votes. The devices were displaying errors that interfered with the ability to collect votes. In order to diagnose the problem, the Department of Elections (ELECT) initiated a review of the devices to identify the cause of the problems. As part of the review, ELECT engaged Commonwealth Security and Risk Management staff in the Virginia Information Technologies Agency (VITA) to perform a security analysis of the devices.

**As a result of the findings included in this report, VITA recommends discontinuing use of the Advanced Voting System WINVote devices. The security review determined that the combination of weak security controls used by the devices would not be able to prevent a malicious third party from modifying the votes recorded by the WINVote devices. The primary contributor to these findings is a combination of weak security controls used by the devices: namely, the use of encryption protocols that are not secure, weak passwords, and insufficient system hardening.**

Security deficiencies were identified in multiple areas, including physical controls, network access, operating system controls, data protection, and the voting tally process. The combination of critical vulnerabilities in these areas, along with the ability to remotely modify votes discretely, is considered to present a significant risk. This heightened level of risk has led VITA security staff to conclude that malicious third party could be able to alter votes on these devices. These machines should not remain in service.

## Scope

ELECT recently became aware that error messages were appearing on AVS WINVote devices used during a recent election. While the activity did not significantly impact the voting process, the errors on the devices prompted a technical review. As part of that review it was determined that the devices had potential security risks. To evaluate the risks, ELECT requested that VITA security staff investigate security issues on the WINVote devices. VITA was provided 10 Advanced Voting Systems WINVote devices with the following serial numbers: WV002648, WV002683, WV002715, WV002745, WV002797, WV002809, WV002811, WV002812, WV002815, and WV002818. The devices were tested in their default configuration for all phases of the testing.

The goal of testing these devices was to determine whether the security controls on the devices were sufficient to protect voting data from alteration.

## Testing Methodology

VITA attempted to perform security testing by using methods that would allow votes to be altered in an undetectable manner. To accomplish this, VITA utilized commonly documented exploit techniques and

open source platforms. Tests were conducted using the default configuration and devices were not altered for testing. VITA was not provided with any information concerning the existing security controls enabled on these devices, therefore making the review a "black-box" test.

The testing consisted of five parts: physical, network, operating system, data, and vote talley process. VITA attempted to bypass the security controls identified in each of these parts in order to gain access to the part of this device where the voting records were maintained. The following sections describe the steps taken to bypass security controls in each part.

## Physical

The physical security of the device consists of a single locking mechanism that covers the printer and power button. This lock can be easily circumvented, although the access it provides to the device would not allow a device to be compromised without using supplementary equipment. In addition to the universal serial bus (USB) port under the locked cover, the device has two USB ports on the top of the device. These ports are easily accessible and accept standard USB devices. While there are some limitations of the types of devices that can be plugged into the ports without notice, a malicious third party could plug in a device that provides access to the machine either locally or remotely.

As part of testing, VITA accessed each device's basic input/output system (BIOS) and modified the drive boot order. VITA then attached a USB compact disc drive (CD-ROM), and had the system boot from that CD-ROM instead of the internal drives. By doing this, VITA was able to force the system to boot to an alternate operating system (Knopix), and take images of the system drives. This test, as performed, is likely to be noticed; however, it may be possible to use a smaller profile bootable device and access the system discretely. This approach would enable modification of the device if it was discreetly rebooted.

Time constraints prohibited testing of each type of external USB device that could allow local access. However, VITA believes it is probable that an attacker could install a device that would allow remote or local access to monitor, modify, or provide unauthorized access to data.

## Network

One of the most significant concerns involving the WINVote system is the ability to access the devices from a remote location using the Institute for Electronics Engineers (IEEE) 802.11b wireless protocol. The wireless cards on the devices provide an attack vector where an external party can access the WINVote devices and modify the data without notice from a nearby location.

The first part of the wireless testing involved a review of the security used to protect communications between WINVote devices. Each device has a default configuration where wireless communication is configured as peer-to-peer with wired equivalent privacy (WEP) encryption. The devices broadcast their wireless network name (service set identifier, commonly known as the SSID) where it can be easily detected by most devices that have wireless cards.

One additional important note is that while the WINVote application appears to have the ability to disable the wireless network from within the application, it does not disable the network interface on the device. When the wireless network is disabled using the WINVote interface, the application will no

longer seek other devices on the network. Although the application will not find other systems, the device's network card remains online and will send and receive traffic even though the application indicates it is disabled. Based on VITA testing it is not possible to prevent network access by disabling the network using the WINVote application. To determine if wireless functionality could effectively be disabled by other means, VITA performed the following actions:

- Physical removal of the wireless network adapter;
- Disabling the wireless capability through the command line and network control panel;
- Renaming the wireless zero configuration dynamic link library (dll).[1]

Both the physical removal of the wireless adapter and changes to the device software rendered the WINVote device unable to execute and administer an election.

Once VITA identified the wireless network name used by the devices, the next step was to test the encryption used to protect communications. The encryption used was identified as WEP. The WEP algorithm was "deprecated" by the IEEE in 2004 since it had been demonstrated that the algorithm could be exploited by security researchers and because a more secure algorithm, wifi-protected access (WPA2), was available. Because the devices use an insecure algorithm, the use of widely published exploit techniques[2] [3] could allow a malicious third party to identify the wireless password and join the WINVote ad-hoc network.

During VITA's testing of the devices, network communications between two WINVote devices were monitored for approximately two minutes and a packet trace was taken of the wireless network communications. Using this packet trace, it was possible to craft a network packet and use that packet to exploit the weakness in the WEP algorithm to crack the WEP encryption key. This password ("abcde") is classified as weak and could have been quickly identified using common password guessing tools. With that passphrase it was possible to join to the WINVote ad-hoc network with specialized security workstations and start attempting to compromise the WINVote device's operating system.

Once joined to the WINVote ad-hoc network, VITA performed a vulnerability analysis using Nmap and Nessus scans[4] against several of the systems. Results indicated that the systems were not utilizing a firewall and were vulnerable to a number of critical remotely-exploitable vulnerabilities. The following ports were open: 135/tcp, 139/tcp, 445/tcp, 3389/tcp, 6000/tcp and 16001/tcp. There were also eight critical, three high, five medium and two low-risk vulnerabilities identified by the Nessus scan, providing several potential avenues of attack.

## Operating System

The WINVote systems run Windows XP Embedded 2002 as an operating system (OS). This OS is currently supported by Microsoft but is scheduled to go end-of-life on January 12, 2016[5]. Although

[1] https://msdn.microsoft.com/en-us/library/dd143250(v=winembedded.5).aspx
[2] http://www.aircrack-ng.org/doku.php?id=simple_wep_crack
[3] http://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/
[4] See attached report
[5] http://www.microsoft.com/windowsembedded/en-us/product-lifecycles.aspx

patches for the OS have been released, the WINVote devices do not appear to have patches or service packs applied. This puts the OS in a deprecated and therefore vulnerable state. Because of this, the devices are vulnerable to many published exploits, such as vulnerability first identified in 2004, MS04-011[6]. The age of this vulnerability provides confirmation that the devices have not been patched for a number of years.

The approach to testing the OS began with an attempt to access a privileged account. Information from the Nmap and Nessus scans was used to target the file sharing service and the file shares to perform a password guessing (brute-force) attack utilizing the open source tool Hydra[7]. The first account targeted was the local administrative account "Administrator" using a standard wordlist (a list of passwords). The use of a weak password by the devices enabled VITA to crack the password ("admin") for that account almost immediately. Using this account and password, full administrative access to the WINVote operating system was available.

It was possible to access the system with these credentials in two ways. The first method utilized the remote desktop protocol (RDP), which provides a remote interactive version of the WINVote system desktop. The second method was to map to the default network shares – C$, D$, ADMIN$, IPC$ - to transfer data to and from the device. The testing also included an attempt to exploit some of the identified vulnerabilities and run tools that would allow modification of the device. VITA was able to successfully execute commands remotely; however, unfortunately because of the age of the device, most of the standard remote management tools that were available in the testing toolkit would not run on the equipment. VITA security staff members believe that with more time it would be possible to create and execute malicious code on the system that would run in the background or allow for unauthorized access to the system. The level of sophistication to execute such an attack is low.

### Data

The voting databases on the devices would be a primary target for an attacker. The databases contain information, such as the ballot, the voting location, and (most importantly) the number of votes. The databases are Microsoft Access databases and require a password. It is important to note that while there is a password on the database, the database itself is not encrypted. The password on the database provides very limited protection and can be bypassed easily with a hex editor (a specialized tool to edit individual bytes of a file) or identified with a password cracker.

A password cracker was used by VITA to attempt to obtain the password protecting the database. The weak password on the database permitted VITA staff to access it in approximately 10 seconds using "AccessPasswordRetrievalLite" to guess the password ("shoup"). This password was used for all of the database files. With the password, it was possible to copy the database files to the security analysis system, open them and modify the voting data. To validate that the changes were permanent and not overwritten by the application's controls, a hash of the file (MD5 checksum) was taken and validated after the database had been copied back to the WINVote device. The hash values matched, confirming that the altered files remained on the system.

[6] https://technet.microsoft.com/en-us/library/security/ms04-011.aspx
[7] https://www.thc.org/thc-hydra

### Vote Talley Process

The primary goal of the WINVote testing was to identify whether votes could be modified remotely without detection by voting staff. To determine whether this was possible, VITA executed a controlled election with the vote tallies for each candidate noted. Before closing out the election, VITA downloaded and modified the database containing the vote tallies for each candidate on a remote security analysis station connected to the ad-hoc network. This modified database was loaded back onto the WINVote device and the election was closed. The compromised vote tallies were reflected in the closed election results, proving that the vote data could be remotely modified. This process test was performed with the wireless network both enabled and disabled through the WINVote software.

The documentation reviewed by VITA indicated that the system performed integrity checking of the vote cast to ensure it was not modified during the voting process. However, the system did not perform checks to identify whether the file that stores the votes has been modified. This lack of integrity check allows the file to be changed and votes to be modified.

## Conclusion

Because the WINVote devices use insecure security protocols, weak passwords, and unpatched software, the WINVote devices operate with a high level of risk. The security testing by VITA proved that the vulnerabilities on the WINVote devices can allow a malicious party to compromise the confidentiality and integrity of voting data. This conclusion is supported by the following observations made by VITA staff during the security testing process:

- The voting systems utilize very weak passwords:
    - Passwords were less than seven characters and did not meet best practices for complexity (i.e. they consisted of only lower case letters). Cracking these passwords required minimal effort using freely available toolsets.
    - Passwords were consistent across all systems tested and appear to be part of the default configuration. All passwords identified were simple and easily guessed, consisting of either a common pattern (i.e., abcde), a common default password (i.e., admin), or a phrase directly related to the system manufacturer (shoup).
    - The scope of testing did not include the impact of changing the default password. But it does not appear possible to change the wireless password directly on the WINVote device. In addition, the impact to the WINVote application once the passwords were changed is unclear. Possible impacts range from lost communication between systems to the inability to record votes properly.
- The voting systems utilize a deprecated, insecure wireless encryption algorithm – wired equivalent privacy (WEP):
    - WEP was superseded by the wifi-protected access (WPA) algorithm in 2003 because of security concerns. The IEEE declared WEP as vulnerable to compromise in 2004.
    - By capturing and analyzing approximately two minutes of wireless traffic between two voting devices, it was possible to craft and generate network traffic that facilitated the

cracking of the key for the encrypted traffic. This cracking was performed using freely available toolsets. Once the encryption key was compromised, an attacker could join the wireless ad-hoc network, record voting data or inject malicious data, and/or connect to systems on the network.

- The voting devices are not hardened in accordance with best practice[8]:
  - The systems are running an unpatched and vulnerable operating system – Windows XP Embedded 2002. No apparent service packs or patches have been applied to the systems, indicating that they had likely not been patched since initial acquisition or last certification. The systems are vulnerable to a number of critical vulnerabilities that can be exploited to allow remote access to the system.
  - The devices are not running standard security software such as firewalls or anti-malware software and do not restrict access to exploitable services (RPC[9], DCOM[10] and terminal services).
- The WINVote databases that maintain voting data, while password protected, are not encrypted and can be modified using freely available editors without knowledge of the password. Access to this database allows modification of the voting data.

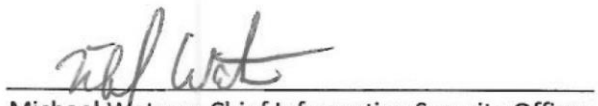
## Recommendation

VITA recommends that the Advanced Voting Systems WINVote devices not be used in future elections.

[8] https://www.sans.org/critical-security-controls/control/20
[9] https://msdn.microsoft.com/en-us/library/windows/desktop/ms691207%28v=vs.85%29.aspx
[10] https://technet.microsoft.com/en-us/library/cc958799.aspx

## Approvals

This report was prepared by the Virginia Information Technologies Agency and presented to the Department of Elections on 4/14/2015.



Michael Watson, Chief Information Security Officer
Executive Director, Commonwealth Security and Risk Management

Date