MACOMB COUNTY
1818
MICHIGAN

Anthony G. Forlini

Macomb County Clerk
Register of Deeds

Kathy Smith
Chief Deputy Clerk

Jennifer Walker
Deputy Register of Deeds

January 6, 2022

The Macomb County Clerk's Office initiated a forensic audit of the county election servers. This was done for our office to develop better methods for high quality elections in the future, address concerns of the past and to bolster confidence in future elections.

As a result of the audit dated January 5, 2022, we learned that there was no outside interference in our election server, our election software, as well as our modem communication systems.

This was just one step to restore confidence in the election process. In addition, the Clerk's Office is taking steps to improve the overall integrity of our system. Macomb County's Information Technology Department will oversee computer configurations and settings to ensure data is properly protected. We will require local clerks to physically bring in tabulator memory sticks, avoiding the possibility of modem vulnerabilities. We will also be "HASH" validating our server for every election.

As the following report indicates, all related computer files matched the verified "HASH" values from SLI Compliance for the ES&S System, no evidence of malicious internet connectivity was found, only proper zero tunnel connections were made, and no evidence of malicious or unexpected activity was detected on the systems.

As always, we intend to stay vigilant and keep abreast of changes with the ever changing world of technology.

Tony

Anthony G. Forlini
Macomb County Clerk

PRO V&V

VERIFICATION VALIDATION

Forensic Audit Report

Macomb County Michigan Audit of the Election Systems & Software (ES&S) EVS 6050 Voting System

Approved by: Ryan Jackson Cobb

Digitally signed by
Ryan Jackson Cobb
Date: 2022.01.05
11:38:04 -06'00'

Jack Cobb, Laboratory Director

January 5, 2022

Disclaimer: This campaign was tested by an EAC accredited VSTL to applicable standards of the VVSG. All testing and references were performed outside of the EAC Test and Certification Program.

v. TR-01-03-MAC-01.02

1.0 INTRODUCTION

The purpose of this report is to document the procedures that Pro V&V, Inc. followed to perform a forensic audit of the Election Systems & Software (ES&S) EVS 6.0.5.0 Voting System for Macomb County Michigan. Pro V&V has prepared this report as a summary of forensic auditing efforts as detailed in Pro V&V Quotation No. 01-03-MCM-2021-01.

This effort included verification of the following items:

1. Verifying that the software installed on the county back office election servers is the same as the software certified by the U.S. Election Assistance Commission and the State of Michigan.
2. Verifying that no malicious software is running on the components.
3. Verifying that the components were properly connected to the dial-up zero tunnel private network and were not maliciously connected to any other network..
4. File and activity analysis. Verify no files were maliciously manipulated either manually or electronically through file and activity analysis.

1.1 References

The documents listed below were utilized in the development of this Report:

- Pro V&V Quotation No. 01-03-MCM-2021-01
- Election Assistance Commission Testing and Certification Program Manual, Version 2.0
- Election Assistance Commission Voting System Test Laboratory Program Manual, Version 2.0
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2020 Edition, "NVLAP Procedures and General Requirements (NIST Handbook 150)", dated July 2020
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2017 Edition, "Voting System Testing (NIST Handbook 150-22)", dated July 2017
- Pro V&V, Inc. Quality Assurance Manual, Version 6.0

1.2 Terms and Abbreviations

The terms and abbreviations applicable to the development of this Test Report are listed below:

"EAC" – United States Election Assistance Commission

"EMS" – Election Management System

"ESS" – Election Systems & Software

"QA" – Quality Assurance

"VSTL" – Voting System Test Laboratory

1.3 Background

Macomb County Michigan Elections Office contracted with Pro V&V to conduct a forensic audit of the deployed backoffice configuration components of the EVS 6.0.5.0 Voting System. These components are used to operate the election management system (EMS) that provides end-to-end election management activities for EVS6050. These activities include pre-election functions for creating the election, defining contests, candidates and ballot formats and performing post-election results processing including accumulating, tallying and reporting election results.

The components evaluated were the EMS Server, DataCom Server, and three EMS Workstations components.

1.4 System Description

ES&S Voting System 6.0.5.0 (EVS6050) is a modification to the previous EAC certified ES&S Voting System 6.0.4.0 (EVS6040) release. EVS6050 has previously been VSTL-tested and certified for use in the State of Michigan.

1.5 Audit Details

The evaluation consisted of the following tasks:

- Set up the forensic environment
- Complete Chain of custody provisions for transfer of equipment between Macomb County and Provider
- Conduct an inventory of the systems, take pictures, record serial numbers, examine tamper evident seals
- Disassemble EMS Server to access storage media (hard drives), take pictures and record hard drive orders of raid drives
- Image server hard drives
- Imaging workstation hard drives
- Copy created images
    - One used for analysis

    - One used for chain of custody / archival requirements

- Analysis
    - Verification of system hashes
    - Compare EAC certified listing of expected software against software installed
    - Malicious software analysis / scanning using multiple signature-based Virus/malicious software detection software
    - Internet connectivity analysis
    - Variable analysis work
        - File and activity Analysis: in-depth analysis of File system Changes to the HDD volume, analysis of time and frequency of applications run on the systems
        - Images/file analysis of potentially deleted images or files
        - Registry analysis
        - Deleted file/evidence recovery

1.6 General Information

The on-site cloning of the components was performed by Pro V&V on-site under the observation of Ben Cotton of CyFIR and Oscar Carretero of Cadre Information Security at the Macomb County Michigan Elections Department located at 32 Market Street, Mount Clemens, MI 48043. During the cloning process, Pro V&V retained complete physical access to all EMS components.

The audit and evaluation was conducted under the guidance of Pro V&V by personnel verified by Pro V&V to be qualified to perform the evaluation. Testing was conducted at the Pro V&V test facility located in Cummings Research Park in Huntsville, Alabama. Pro V&V currently maintains custody of all clones and images.

2.0 AUDIT OVERVIEW AND RESULTS

The audit process included creation of raw disk clones using a bit-to-bit copy of each item of system media. Two additional images were created by Pro V&V in Huntsville, Alabama, one for archival purposes and one for analysis. This allowed the examiners to audit and analyze the components without compromising the original system environments and original clone discs. Once the system media was imaged, the examiners used forensic tools to inspect the systems for indicators of internet connectivity and malicious or unauthorized software present on the systems.

The evaluation addressed each of the previously stated verification objectives in the following manner:

Table 2-1: Testing Overview

Objective #	Test Objective	Test Evaluation
1	**Verifying that the software installed on the county back office election servers is the same as the software certified by the U.S. Election Assistance Commission and the State of Michigan.**	Examination for Item #1, verification of hashes, included usage of: • Verification scripts and procedures from SLI Compliance.
2	**Verifying that no malicious software is running on the components.**	Examination for Item #2, checking for malicious software, included usage of: • Bitdefender (Antivirus Free Edition 1.0.21.270, Engine version: 7.90247) • Malwarebytes (Version 4.4.10.144, Update package version 1.0.47301, Component package version 1.0.1499) • Microsoft Defender Antivirus (Antimalware Client Version 4.18.2110.6, Engine Version 1.1.18700.4, Antivirus Version 1.353.1153.0, Antispyware Version 1.353.1153.0) • OSForensics (Version 9.1.1001)
3	**Verifying that the components were properly connected to the dial-up zero tunnel private network and were not maliciously connected to any other network.**	Examination for Item #3, internet connectivity check, included usage of: • Manual review utilizing OSForensics.
4	**File and activity analysis. Verify no files were maliciously manipulated either manually or electronically through file and activity analysis.**	Examination for Item #4, file and activity analysis, included usage of: • Manual review utilizing OSForensics.

2.1 Summary Findings

2.1.1 Objective 1

Verifying that the software installed on the county back office election servers is the same as the software certified by the U.S. Election Assistance Commission and the State of Michigan.

Summary Findings:

Each of the four EMSs and DataCom server that were examined were first bit-by-bit imaged. The images were then mounted read-only for file verification. This allowed the examiners to maintain a clean snapshot of the EMS client systems under evaluation.

All related files matched the verified hash values from SLI Compliance for the ES&S System.

In addition, a sample of the application logs that were loaded into the postgress database were reviewed and it was verified that no abnormal entries from normal operational use were present. It must be noted that 156 of the tabulator removable media of the 397 were available from the November 2020 election.

2.1.2 Objective 2

Verifying that no malicious software is running on the components.

Summary Findings:

All files on each of the EMSs and DataCom server were examined to determine if any malicious files were resident. Three different antivirus scanners were utilized (Bitdefender, Malwarebytes, and Microsoft Defender Antivirus), along with OSForensics, to examine the contents of each component. In addition to using multiple forms of antivirus and malicious software detection software, manual examination of the systems was conducted to identify malicious or unauthorized software on the systems. These inspections included:

- *Inspection of operating system artifacts. This included items such as most recently used objects, installed programs, event logs, and recycle bin.*
- *Inspection of internet artifacts. Including items such as downloads, browser history, form history, and bookmarks.*
- *Inspection of external device usage. Includes history of USBs, mounted volumes, and mobile backups.*

No instance of malicious software was found on any of the devices.

2.1.3 Objective 3

Verifying that the components were properly connected to the dial-up zero tunnel private network and were not maliciously connected to any other network.

Summary Findings

OSForensics was used to examine the activities of each EMS component and DataCom server, looking to determine if any connections were made to the internet. OSForensics software was used to inspect the systems to identify if there were any instances of the systems being connected to an internet routed network. These inspections included:

- *Inspection of operating system artifacts. This included items such as event logs, UserAssist entries, jump lists, and shellbags.*

- *Inspection of internet artifacts. Including items such as website logins, chat logs, peer-to-peer, and WLAN connections.*

- *Inspection of external device usage. Includes history of USBs, mounted volumes, and mobile backups*

No evidence of malicious internet connectivity was found. Only proper zero tunnel connections were made.

2.1.4 Objective 4

File and activity analysis.

Summary Findings

OSForensics was used to examine the file system activities of each EMS component and DataCom server, looking to determine if anything seemed inconspicuous. These inspections included:

- *Inspection of user activity. This included items such as recycle bin, shellbags, jump lists, UserAssist entries, and event logs.*

- *Inspection of deleted files. These are deleted files no longer in the recycling bin.*

No evidence of malicious or unexpected activity was detected on the systems.

3.0 RECOMMENDATIONS

At audit completion, Pro V&V developed the following recommendations based on the findings:

- During the on-site cloning it was noticed that one of the hard drives in the EMS RAID was orange indicating that one of the six hard drives were bad. It should be noted that no data was lost due to the system redundancy achieved with the EMS being set to RAID 1. It is recommended for the election staff to routinely do a visual inspection of the server every time the passwords on the workstation clients are updated.

- During the analysis conducted in the Pro V&V lab, the EMS data RAID was set to RAID 1. In this configuration drives three and four are not being used. However, the RAID could be configured to RAID 5, utilizing all the hard drives in the EMS server expanding system redundancy.

- During the analysis of the application logs, it was noticed that there were only two logins being used for the EMS workstations and Server. Best practices is each workstation should have its own username and password so that the logs will tie an individual device to a log entry.

- All logs from tabulators were not present for the audit. All USB sticks from the tabulators should be loaded into the EMS components to add an additional verification of the results. It should be noted that all USB sticks were collected from the August 2021 election.

A detailed technical report is provided under separate cover.