NEW YORK STATE | Homeland Security and Emergency Services | Counter Terrorism | Cyber Incident Response Team

State Board of Elections

ePollbook Testing Full Report

May 22nd, 2019

Contents

[redacted]

Executive Summary

The New York State Board of Elections (SBOE) will be implementing an electronic pollbook solution (ePollbooks) for use during the upcoming 2019 election period and beyond. To support this initiative, the DHSES Cyber Incident Response Team (DHSES CIRT) provided specific security testing on each vendor ePollbook system that was submitted for consideration by SBOE.

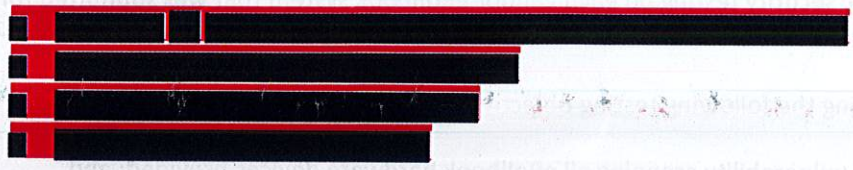
DHSES was responsible for performing the following testing objectives:

- Perform non-authenticated vulnerability scanning all ePollbook hardware devices provided; and
- Validate data confidentiality is maintained during both external data transmissions to a vendor cloud service, and data transmissions between two ePollbooks connected to the same local network.

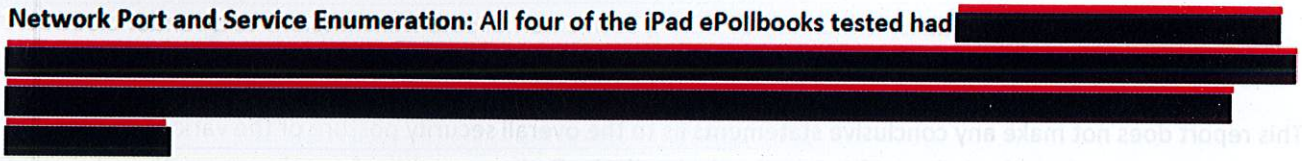
This report does not make any conclusive statements as to the overall security posture of the various vendor ePollbook submissions and technical solutions. This report only details the findings resulting from the completion of the outlined testing objectives.

Vendor 1: KNOWiNK

- **Hardware Tested:** The following list details the hardware components submitted by the vendor that were included in the DHSES CIRT testing:



- **Network Port and Service Enumeration:** All four of the iPad ePollbooks tested had



  - Please refer to the following supplemental support files for full Nmap scanning results:
    - KNOWiNK/PB1/ Top-SYN-TCP-PB1.nmap
    - KNOWiNK/PB1/ Top-UDP-PB1.nmap
    - KNOWiNK/PB1/Aggressive-Scope-SYN-TCP-PB1.nmap
    - KNOWiNK/PB2/ Top-SYN-TCP-PB2.nmap
    - KNOWiNK/PB2/ Top-UDP-PB2.nmap
    - KNOWiNK/PB2/Aggressive-Scope-SYN-TCP-PB2.nmap
    - KNOWiNK/PB3/ Top-SYN-TCP-PB3.nmap
    - KNOWiNK/PB3/ Top-UDP-PB3.nmap
    - KNOWiNK/PB3/Aggressive-Scope-SYN-TCP-PB3.nmap
    - KNOWiNK/PB4/ Top-SYN-TCP-PB4.nmap
    - KNOWiNK/PB4/ Top-UDP-PB4.nmap
    - KNOWiNK/PB4/Aggressive-Scope-SYN-TCP-PB4.nmap

- **Vulnerability Scanning:** No critical, high, medium, or low vulnerabilities were identified on any of the four iPad ePollbooks scanned.

  - Please refer to the following supplemental support files for Nessus vulnerability scanning results:
    - KNOWiNK/PB1/Basic-KNOWiNK-PB1-5-8.html
    - KNOWiNK/PB2/Basic-KNOWiNK-PB2-5-8.html
    - KNOWiNK/PB3/Basic-KNOWiNK-PB3-5-8.html
    - KNOWiNK/PB4/Basic-KNOWiNK-PB4-5-8.html

- **Data Transmission Confidentiality:**
  - Data confidentiality is being maintained for external / outbound Internet traffic destined for the vendor's cloud service using [redacted] encrypted tunnels.

[redacted]

NEW YORK STATE | Homeland Security and Emergency Services | Counter Terrorism | Cyber Incident Response Team

State Board of Elections

ePollbook Testing Summary

May 16th, 2019

Contents

[redacted]

Executive Summary

The New York State Board of Elections (SBOE) will be implementing an electronic pollbook solution (ePollbooks) for use during the upcoming 2019 election period and beyond. To support this initiative, the DHSES Cyber Incident Response Team (DHSES CIRT) provided specific security testing on each vendor ePollbook system that was submitted for consideration by SBOE.

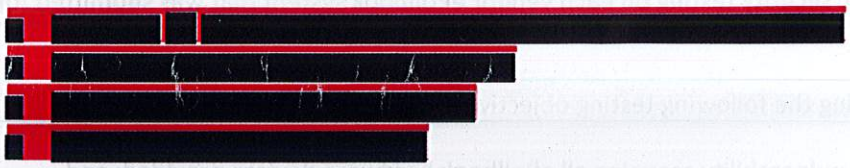
DHSES was responsible for performing the following testing objectives:

- Perform non-authenticated vulnerability scanning all ePollbook hardware devices provided; and
- Validate data confidentiality is maintained during both external data transmissions to a vendor cloud service, and data transmissions between two ePollbooks connected to the same local network.

This report does not make any conclusive statements as to the overall security posture of the various vendor ePollbook submissions and technical solutions. This report only details the findings resulting from the completion of the outlined testing objectives.

Vendor 1: KNOWiNK

- **Hardware Tested:** The following list details the hardware components submitted by the vendor that were included in the DHSES CIRT testing:



- **Network Port and Service Enumeration:**

- **Vulnerability Scanning:** No critical, high, medium, or low vulnerabilities were identified on any of the four iPad ePollbooks scanned.

- **Data Transmission Confidentiality:**
  - Data confidentiality is being maintained for external / outbound Internet traffic destined for the vendor's cloud service using encrypted tunnels.

  - Data confidentiality is being maintained for peer-to-peer traffic between two pollbooks using encrypted tunnels.

- **Wireless Network Configuration:** All three of the mobile cellular hotspots submitted by the vendor utilized