Unisyn Response to Election Security Researcher Forum Findings

03/01/2024

Introduction:

In September 2023, the IT-ISAC's Election Industry Special Interest Group (EI-SIG), facilitated the Election Security Research Forum (ESRF). Hosted at MITRE Corporation's National Election Security Lab, the ESRF was a pilot program that provided the opportunity for qualified security researchers to engage with modern, pre-deployment (uncertified) voting technology provided by IT-ISAC Election Industry SIG members Election Systems & Software (ES&S), Hart InterCivic, and Unisyn Voting Solutions. All companies and researchers agreed to participate under the terms of Coordinated Vulnerability Disclosure (CVD). This document represents the response from Unisyn Voting Solutions (Unisyn) to those security researchers that were kind enough to submit written responses to Unisyn explaining and suggesting remediations for their findings.

Potential Attack #1

Attempted stuffing of collapsible ballot box

Description: Two researchers spent time and effort pulling and forcing the locked rear steel door of the collapsible ballot box to separate slightly from the steel frame of the ballot box. This allowed enough gap between the door and frame to be able to inset additional ballots.

Unisyn Response: Unisyn determined that the risk related to this attack was low. This determination was made because the amount and type of physical force needed to alter the fit of the ballot box door and frame would absolutely draw attention in a real-world election environment, and the evidence of the attack was clear from the bent door and ballot box frame. Unisyn began addressing the ballot box rigidity and flex issues even before the Researcher Event. Unisyn has developed and are working on the tooling for a new, rigid/hard ballot box that will allow less flex, no matter how much force is used. In addition, we will review the current lock mechanism to see if we can make it tighter on the new box. Although not present at the Researcher Event, an internal e-bin has already been developed and implemented as a separate smaller internal box/bin for the collapsible box used during the event.

Potential Attack #2

Multi-Vote with a single ballot (fishing method)

Description: Researchers were able to scan a ballot on the FVS scanner and then pull the ballot back out with a long piece of adhesive tape attached to the ballot. The adhesive tape was used to pull the ballot back out of the machine during the split second that the vote was being scanned/processed. Timing was critical here, and while it did not work every time, it was successful on many instances. During successful attempts at this attack, the vote was counted, but the physical ballot stayed in the hands of the attacker, potentially allowing them to submit the ballot more than once.

Unisyn Response: Unisyn determined that the risk of this potential attack in a polling place environment was low. Much like some of the other physical attacks, election officials are trained to notice unauthorized/unusual behavior, and a voter/attacker applying a long strip of adhesive tape to a ballot would certainly fall outside normal polling place protocols. Unisyn continues to work with our scanner vendor to determine if we can tighten the feed rollers so that a ballot cannot be dragged out by any method without causing noticeable damage to the ballot.

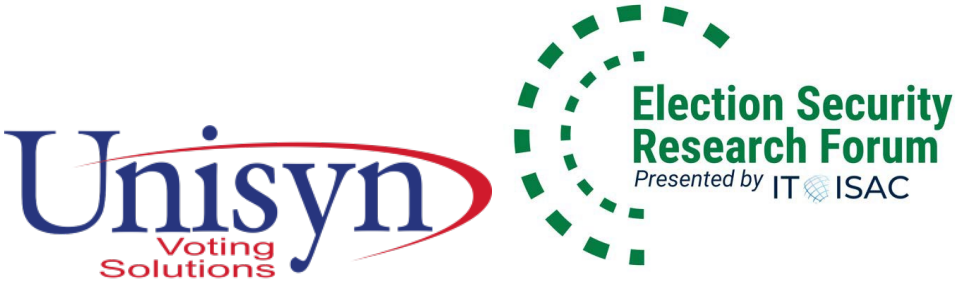
Potential Attack #3

Forcing locking mechanism of scanner cover

Description: Researchers were able to open the locked cover of the ballot scanner on the FVS by flexing the plastic to move the locking mechanism over the lock's catching edge.

Unisyn Response: Unisyn determined that this potential attack risk was low. In a polling place scenario, an attacker/voter would definitely be noticed leveraging the scanner cover of the optical scan device with the effort required in order to disengage the lock. Unisyn engineers have identified that the plastic flats that hold the lock in position could be forced to over-rotate, thereby defeating the lock. A metal anti-rotation bracket has been added to fix the lock in the proper orientation that stops the lock from being over-rotated.

The remaining researcher attacks noted below in this report were undertaken only after Unisyn gave the researchers permission to access the scanner passwords and decompose and disassemble the unit into individual components.



Potential Attack #4

Maintenance user

Description: After accessing the FVS hard drive via connection to a separate researcher laptop via, it was determined that an additional maintenance user was present, although unused.

Unisyn Response: Unisyn determined that the potential risk of this attack is low because of various physical and logical safeguards on the system, i.e., prevention of connection peripheral devices and the lack of access to a command line or log in. Additionally, the maintenance user is purely diagnostic in function and has limited rights and privileges, belonging to the "wheel" group. NIST SCAP best practices recommends the existence on one wheel group user to access the system for diagnostics other than root. Unisyn has reviewed the OS configuration **and** determined that there are no further/other unused maintenance credentials present. Unisyn will review the function in future releases to see if it needs to exist at all.

Potential Attack #5

Accessible USB attached to monitor touchscreen

Description: The researcher found a USB cable plugs into the back of the FVS screen; the area of the plug is covered by a screwed-on panel that had already been broken off by the time the researcher saw the machine and determined, given its condition, that this attack could be executed.

Unisyn Response: Unisyn has determined that the risk of this potential attack is low, considering that gaining access to this component to perform any modification would require destructive access to the system that would be immediately recognizable by a layperson, much less a trained individual**.** Unisyn is currently looking into better ways to connect the monitor and to more completely secure the USB.

Potential Attack #6

BIOS password is not unique

Description: The FVS BIOS is locked out via password, but the same password is used on all devices because unique passwords introduce a legitimate and significant system maintenance nightmare. However, physical access on a single system could brute-force it without touching any tamper seals, or OS-level access could dump the bios via software to reverse engineer it.

Unisyn Response: The potential risk of this issue is low due to the BIOS password policy followed by Unisyn. Unisyn is still looking at options for even greater security on the BIOS password. Per-device

password based on system serial number or similar – even if not cryptographically secure – would at least make automating an attack more difficult. Unisyn understands that per-device passwords would be problematic to realistically implement in a real-world election scenario.

Potential Attack #7

Ran custom CentOS volume which was unencrypted

Description: As stated, the rest of the product, including where the software resides, is on an encrypted partition with a key that is stored within the TPM of the device. This is determined to be a low risk, both for the above reason, and that gaining access to the hard drive to perform any modification would require destructive access to the system that would be immediately recognizable by a layperson, much less a trained individual.

Unisyn Response: Unisyn is exploring strategies for providing full disk encryption on all future products, while not impacting efficiency of the manufacturing process.

Potential Attack #8

Any USB anomalies should flag the software

Description: If the election provisioning USB is removed at any time, the system stops the election; the same should be true for any USB device since there is no use case where devices should change mid-election.

Unisyn Response: There are actually several use cases where the effective recovery of a USB device (printer/scanner/touchscreen) is required. That said, the system is looking for specific devices and will not communicate with anything unexpected. Future versions will apply more stringent rules by whitelisting USB components and flagging anything that does not match criteria, and making sure invalid attempts are logged. The system already applies protections and limitations on connected devices consistent with the NIST SCAP best practices.

Potential Attack #9

USB protocols not present during BIOS

Description: Even if the two external USB ports are locked out by the OS, they are still likely enumerated and used by the BIOS. Once the BIOS password has been defeated, it may be feasible to connect a keyboard and storage device (or malicious/discrete custom hardware), to modify secure boot settings

and boot alternative media, or, more maliciously, disable secure boot, make modifications to the factory OS (depends on bypassing FDE if present), and boot it without secure boot turned on.

Unisyn Response: As noted, any attacks in this vein first require defeating the BIOS, which will be mitigated as stated in #7. Unisyn is exploring possible options for the BIOS which will additionally mitigate, but there are use cases where booting to external device is required, however, so prevention of this feature is not viable. But as stated, there are physical protections to ensure the ports are not accessed by unauthorized personnel.

Conclusion

As Unisyn and the other manufacturers participating in this Research Forum have noted, Federal and State certification procedures are currently an impediment to getting vulnerability remediations into the field in any reasonable timeframe. The voting industry is currently working with the U.S. Election Assistance Commission (EAC) and State entities to develop new procedures that would permit the implementation of a true coordinated vulnerability disclosure program for this industry. In the meantime, Unisyn will submit the above noted fixes/remediations during our next regular certification effort with the EAC.