COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

J. Alex Halderman • Professor

August 23, 2022

John Poulos
Dominion Voting Systems

cc: Robert Giles, Nick Ikonomakis

Subject: Privacy Flaw Affecting Dominion ICP and ICE Tabulators

Dear Mr. Poulos:

We have identified a serious privacy flaw that affects data produced by ImageCast Precinct (ICP) and ImageCast Evolution (ICE) tabulators. Using information that many of your customers make public, such as cast-vote records (CVRs) or ballot images, an attacker can ascertain the order in which all ballots on a machine were cast. In many cases, this would allow attackers to determine how identifiable individuals voted.

Dominion tabulators assign every scanned ballot a record ID number, which, together with tabulator and batch IDs, uniquely identifies each ballot in an election. The record IDs appear in several forms of data produced by the Democracy Suite EMS, including exported CVRs and ballot image filenames, both of which many localities routinely publish or treat as public records subject to FOIA. Democracy Suite documentation states that exported CVRs entail "[n]o compromise to voter privacy",[1] which implies that the record IDs they contain are intended not to be traceable to specific voters.

However, the method that the ICP and ICE use to generate record IDs is flawed.[2] Each model follows a fixed sequence of one million six-digit numbers. The only parameter that differs from one tabulator or batch to the next is the starting point within the sequence. If an attacker knows the entire sequence, it is a simple matter to determine the order in which all ballots were cast given only the set of record IDs for a batch.

Using only public information, we were able to deduce the complete record ID sequences for the ICP and ICE and the algorithm that generates them. Rather than a cryptographically secure pseudorandom number generator, each is produced by a linear congruential generator—a kind of algorithm that is vulnerable to a variety of well known attacks. The output is then ineffectively obfuscated by a simple substitution cipher and reordering of digits. The steps we took to deduce the algorithm can potentially be performed using only pen and paper, and there is an appreciable risk that malicious parties will deduce it independently from our work.

You can verify that this Python code reproduces the complete record ID sequence for each tabulator:

```
def generate_sequence(p):
    return [sum([5,0,8,3,2,6,1,9,4,7][864803*n//10**p[i]%10]*10**i for i in range(6))
        for n in range(1000000)]
icp_sequence = generate_sequence([2,3,1,5,0,4])
ice_sequence = generate_sequence([1,5,0,4,2,3])
```

[1] https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-RTR-UserGuide-5-11-CO.pdf#page=101

[2] All publicly available ICP and ICE ballot images and CVRs that we have examined suffer from this flaw, and it likely affects all current versions of both devices. The ICC tabulator and ICX DRE do not appear to be affected, based on our present knowledge.

Bob and Betty Beyster Building
2260 Hayward Street, Ann Arbor, MI 48109

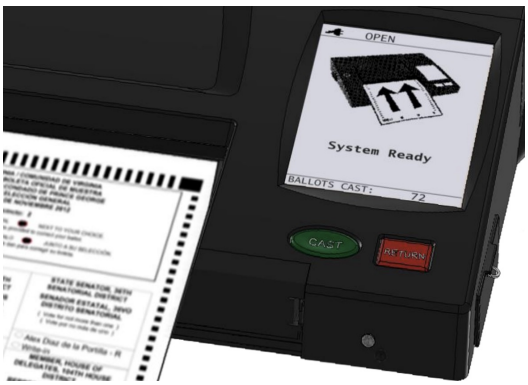
https://**jhalderm.com**
jhalderm@umich.edu

COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

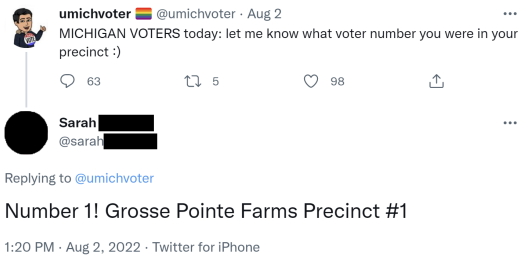
J. Alex Halderman • Professor

We emphasize that the record ID flaw can be discovered and exploited by members of the public without any access to equipment or breach of controls. Here are some examples of circumstances where an attacker could use it to identify how individuals voted:

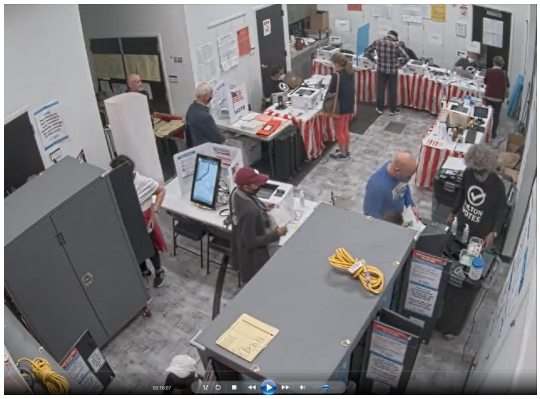
- A voter can determine their own position in the batch by noting the public counter value shown on the tabulator in many jurisdictions, and this reveals the positions of other ballots cast relative to theirs. For instance, if a man's wife uses the scanner just before he does, and it shows the screen at right as he insert his ballot, he learns that her ballot is 72nd in the batch. If CVRs or ballot images are public, he can use the record ID flaw to identify her ballot and see how she voted. Poll workers or observers could similarly note the public counter value, or they could count voters as they use the scanner.



- Some voters publicly disclose their polling places and voter numbers on social media, as in the tweet shown here (we have redacted the voter's last name). In localities that use the ICP or ICE and for which CVRs or ballot images are public, this is sufficient to allow anyone to determine how these people voted, even for *past* elections.



- We have identified some localities where surveillance footage of polling places is recorded and treated as a public record. (The image at right is from a day-long video from a Georgia county, obtained via an open records request by another party prior to our work.) Combined with CVRs or ballot images, this would be sufficient to associate every ballot with footage of the voter casting it. This could be done for any past election that used the ICP or ICE for which such data and video are available to the public.



- Some jurisdictions publish scanner log files from the ICP or ICE. These logs record the exact time at which the scanner accepts a ballot. Combined with the record ID vulnerability, this information can be used to determine the time-of-casting for every CVR and ballot image (subject to the accuracy of the tabulator's clock). This provides an additional route to identify voters' ballots. For example, journalists sometimes film or photograph candidates and other political figures as they vote. Such media is often timestamped and could be used by anyone to deanonymize those individuals' ballots.

Bob and Betty Beyster Building
2260 Hayward Street, Ann Arbor, MI 48109

https://**jhalderm.com**
jhalderm@umich.edu

COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

J. Alex Halderman • Professor

We recognize that public access to election data, including CVRs and ballot images, is an important form of transparency that can help uphold voter confidence. For this reason, it is imperative to provide solutions so that jurisdictions can safely make such data public, both for upcoming elections and for those in the past. Fortunately, the record ID flaw can be corrected without further loss of transparency by appropriately sanitizing data produced from the ICP and ICE. We recommend the process outlined below:

1. Securely encrypt each record ID using an appropriate key unique to the election, tabulator, and batch. This ensures that each batch is shuffled with a unique, cryptographically strong permutation.
2. Replace each record ID in CVRs and ballot image filenames with the encrypted values.
3. Remove unnecessary metadata (e.g., image file creation times), and sort CVR entries and image files. This ensures that any residual sequence information is removed.

We are developing a software tool to help jurisdictions accomplish these steps.

For future elections, the best solution would be to update the ICP and ICE software to replace the record ID generation method with a secure alternative. We would be happy to provide advice concerning such a change or to assist in validating it.

It is important to inform all jurisdictions that use the ICP or ICE about this problem before the November election, when many will likely release additional vulnerable data. **For this reason, we plan to publicly disclose information about the vulnerability in 30 days.** We will also inform appropriate federal agencies prior to public disclosure, and we will contact individual jurisdictions that we know have published exploitable data from past elections, so that they have an opportunity to sanitize it.

We are available to answer your questions as needed, and we would be happy to collaborate in efforts to further develop and disseminate effective solutions for this problem.

Sincerely,

J. Alex Halderman
Professor
Computer Science & Engineering

Braden L. Crimmins
Graduate Student Research Assistant
Computer Science & Engineering