Central Count Location

TX Vote Collection Server

GA Vote Collection Server

MA Vote Collection Server

Hacker creates a false vote count and modifies source address so the receiving network believes false information is from a legitimate network.

ICMP redirection is exploited by attackers and instead of sending vote count information to the correct device in a more efficient manner, sends it to another device where the votes will be discarded.

An attacker shuts down the network that receives vote count from different areas, so voting stations cannot send information.

An attacker alters DNS records so workers believe they are sending vote counts to the legitimate source [Their states vote collection center] when they are actually sending them to a fraudulent site.

Attackers change public transportation routes to make it harder for voters to access polling location sites.

Attackers post incorrect information online regarding polling locations through their own platforms or by hacking into government run platforms

Polling Station

Employee/Volunteer Logs

Not logging when employees/volunteers are working makes it harder to trace source of attacks

The attacker modifies logs so certain workers appear to be working when they aren't (can link specific workers to attacks they weren't involved in) and vice versa

Different Polling Locations

Steals someone's identification to vote

Austin, TX (photo ID requested not required)

Steals a deceased relative's identification to vote

Atlanta, GA (strict photo ID required)

Falsely identifies as another person to vote

Boston, MA (no documents required)

Declaring to be a volunteer/employee that checks voter identification allowing clearly stolen IDs to pass

Declaring to be a volunteer/employee that places ballots into the voting machine

Claims to have counted a stash of ballots when they didn't or discards ballots so they don't get counted

Declaring to be an IT worker

Vote Counting System

Supplies false vote counts that the system interprets as valid

Tampers with the vote counting system/machine and gives access to hackers/troublesome employee

Attacker shuts down the vote-counting machine - ballots now must be counted by hand

Database containing tallied vote counts set to write instead of read; attackers are able to change data files containing vote counts

Attacker fills up vote count database to max capacity by sending in mass records of fake vote counts

Attacker changes the code/method that increments ballot counts for a specific candidate (could be in favor or against a candidate; changing the code to increment more than one or less than one)

Vote count system code relies on files that have write permissions. These files could be edited or new ones could have been added

Volunteers/employees are able to access voting counts and change them

Specific volunteers are able to access rooms where sensitive data is kept

Does not perform/performs weak authorization to access ballot counting machines

Employees are all given the same level of access across the system when the access level should be specific to employee role

TALLIED VOTE COUNT

IT employee accidentally leaves their account unlocked enabling an attacker inside the voting count system

Attacker breaks in and steals memory disk that contains all information storing vote counts; no backup is available

Employee claims to have not clicked on suspicious link that allowed hackers into system when they did

Uses another employee's login/authentication information to access the vote counting machines/system