Voting Machine vulnerabilities

- **Technical Malfunctions**: Voting machines, like any technology, can malfunction. This could result in votes not being recorded or counted correctly.
- **Hacking**: There's a risk that voting machines could be hacked, potentially allowing someone to manipulate the vote count or disrupt the voting process.
- **Lack of a Paper Trail**: Some voting machines do not produce a paper record of votes, which can make it difficult to audit the results or resolve disputes about the outcome.
- **User Errors**: Voters could make mistakes when using the machines. For example, they might accidentally select the wrong candidate or not understand how to cast their vote.
- **Accessibility Issues**: Some voters, particularly the elderly or disabled, might have difficulty using the machines.
- **Dependence on Electricity**: Voting machines require electricity to operate. Power outages or other disruptions could therefore interfere with voting.
- **Limited Availability**: There might not be enough machines available, leading to long lines and wait times at polling places.
- **Cost**: Voting machines can be expensive to purchase, maintain, and update. This could be a significant burden for some jurisdictions.
- **Outdated Technology**: Some jurisdictions use older voting machines that might not have the latest security features or might be more prone to malfunctions.

Click this link for more information.