Report on Dominion Voting Machines Proves 'Most Secure Election in History' Was a Lie

Description

USA: A highly anticipated report issued Friday by the Cybersecurity and Infrastructure Agency, also known as CISA, is providing official documentation of the major security flaws posed by Dominion Voting Systems Machines. It comes nearly two years after the 2020 presidential election, which the agency had called the "most secure election in history."

While the CISA report states that it has "no evidence that these vulnerabilities have been exploited in any elections," it nonetheless highlights at least nine concrete, alarming security vulnerabilities. The CISA report was issued based on the analysis of J. Alex Halderman of the University of Michigan, and Drew Springall of Auburn University.

The report states that the security advisery affects the following versions of the Dominion Voting Systems ImageCast X software are known to be affected (other versions were not able to be tested): ImageCast X firmware based on Android 5.1, as used in Dominion Democracy Suite Voting System Version 5.5-A and ImageCast X application Versions 5.5.10.30 and 5.5.10.32, as used in Dominion Democracy Suite Voting System Version 5.5-A.

The vulnerability overview lists nine different security concerns. It is important to go beyond the advisery document itself to get a clear picture of the vulnerability. The security vulnerabilities justify the concerns of election observers who pointed out that admin rights could be used to override security features and that the system could potentially be hijacked due to "spoofing."

The security vulnerabilities are listed below:

- The tested version of ImageCast X does not validate application signatures to a trusted root certificate.
- The tested version of ImageCast X's on-screen application hash display feature, audit log export, and application export functionality rely on self-attestation mechanisms. An attacker could

leverage this vulnerability to disguise malicious applications on a device.
- The tested version of ImageCast X has a Terminal Emulator application which could be leveraged by an attacker to gain elevated privileges on a device and/or install malicious code.
- The tested version of ImageCast X allows for rebooting into Android Safe Mode, which allows an attacker to directly access the operating system. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.
- The tested version of ImageCast X can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS.
- Applications on the tested version of ImageCast X can execute code with elevated privileges by exploiting a system level service. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.
- The authentication mechanism used by technicians on the tested version of ImageCast X is susceptible to forgery. An attacker with physical access may use this to gain administrative privileges on a device and install malicious code or perform arbitrary administrative actions.
- The authentication mechanism used by poll workers to administer voting using the tested version of ImageCast X can expose cryptographic secrets used to protect election information. An attacker could leverage this vulnerability to gain access to sensitive information and perform privileged actions, potentially affecting other election equipment.
- The authentication mechanism used by voters to activate a voting session on the tested version of ImageCast X is susceptible to forgery. An attacker could leverage this vulnerability to print an arbitrary number of ballots without authorization.

CISA recommended the following recommendations as ‘mitigation’ measures:

- Contact Dominion Voting Systems to determine which software and/or firmware updates need to be applied. Dominion Voting Systems reports to CISA that the above vulnerabilities have been addressed in subsequent software versions.
- Ensure all affected devices are physically protected before, during, and after voting.
- Ensure compliance with chain of custody procedures throughout the election cycle.
- Ensure that ImageCast X and the Election Management System (EMS) are not connected to any external (i.e., Internet accessible) networks.
- Ensure carefully selected protective and detective physical security measures (for example, locks and tamper-evident seals) are implemented on all affected devices, including on connected devices such as printers and connecting cables.
- Close any background application windows on each ImageCast X device.
- Use read-only media to update software or install files onto ImageCast X devices.
- Use separate, unique passcodes for each poll worker card.
- Ensure all ImageCast X devices are subjected to rigorous pre- and post-election testing.
- Disable the “Unify Tabulator Security Keys” feature on the election management system and ensure new cryptographic keys are used for each election.
- As recommended by Dominion Voting Systems, use the supplemental method to validate hashes on applications, audit log exports, and application exports.
- Encourage voters to verify the human-readable votes on printout.
- Conduct rigorous post-election tabulation audits of the human-readable portions of physical

ballots and paper records, to include reviewing ballot chain of custody and conducting voter/ballot reconciliation procedures. These activities are especially crucial to detect attacks where the listed vulnerabilities are exploited such that a barcode is manipulated to be tabulated inconsistently with the human-readable portion of the paper ballot. (**NOTE:** If states and jurisdictions so choose, the ImageCast X provides the configuration option to produce ballots that do not print barcodes for tabulation.)

It should be noted that a number of these mitigation measures were not followed during the 2020 presidential election. These include ensuring physical security of machines and equipment, as demonstrated by lost flash drives; broken chain-of-custody procedures (ballot drop boxes often led to such violations of election law); machines proven to have been connected to the Internet; missing or destroyed ballot images; and the use of QR Codes rather than human-readable vote printouts.

Thus, CISA's infamous claim that the 2020 election was "most secure in American history" is clearly disproven by its own report two years after the fact.

"While we know there are many unfounded claims and opportunities for misinformation about the process of our elections, we can assure you we have the utmost confidence in the security and integrity of our elections, and you should too," the statement said. "When you have questions, turn to elections officials as trusted voices as they administer elections."

But the election security officials issued such a blasé pronouncement without possibly being able to know all the facts about the 2020 election. CISA can claim that it has no evidence of voting machines being exploited, but voters are left to wonder if that is because it didn't seriously look. After all, CISA is only admitting now that all of voters' concerns about the poor security of Dominion voting machines were valid. Yet, all of these concerned voters have been smeared as 'conspiracy theorists' for years. It turns out that they were right to be concerned.

by Becker News

Category

1. Crime-Justice-Terrorism-Corruption
2. Freedom-Free speech-Resitance & H-rights
3. Main
4. Politics-Geopolitics-Gov.-Events

Date Created
06/06/2022