CISA Report Found Massive System Vulnerabilities In Dominion Voting System In Georgia, But Later Claimed There Wasn’t Evidence Of Abuse Of Vulnerabilities In 2020 Election!

Description

USA: Before the 2020 election, leaders in the government confirmed that the US election would be the safest in US history. We could see major league corrupt actors in the US on the list.

However, the announcement wasn’t backed by real support.

Right after the election, it was found a major security breach with SolarWinds Orion products used by the Dominion Voting Machines. At the same time, an investigation happened in Georgia of the Dominion voting machines used there. The person who did the investigation didn’t like Trump, so he shared a report covered up by corrupt Obama Judge Amy Totenberg.It’s only another example of judicial overreach and corruption and the cover-up of the 2020 election steal.
This Friday, CISA appeared with a report as a response to the problems found in the Halderman report. CISA report claimed:

‘’ J. Alex Halderman, University of Michigan, and Drew Springall, Auburn University, reported these vulnerabilities to CISA.’’

The report included a number of problems with the election system in 2020 in Georgia. This kind of system would be thrown out and replaced even before being put in use, but we have seen in the past years how inept and unprincipled these state governments could be.

The actors in Georgia, including the Secretary of State and Judge Totenberg, did their best and allowed the Dominion system to remain in place with the material problems found in the Halderman report and described in the CISA report.

Below you can find the list of material weaknesses embedding the Dominion Voting System in Georgia.

NOTE: *Mitigations to reduce the risk of exploitation of these vulnerabilities can be found in Section 3 of this document.*

2.2.1 IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347

The tested version of ImageCast X does not validate application signatures to a trusted root certificate. Use of a trusted root certificate ensures software installed on a device is traceable to, or verifiable against, a cryptographic key provided by the manufacturer to detect tampering. An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media.

CVE-2022-1739 has been assigned to this vulnerability.

2.2.2 MUTABLE ATTESTATION OR MEASUREMENT REPORTING DATA CWE-1283

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.

CVE-2022-1740 has been assigned to this vulnerability.

2.2.3 HIDDEN FUNCTIONALITY CWE-912

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.

CVE-2022-1741 has been assigned to this vulnerability.

2.2.4 IMPROPER PROTECTION OF ALTERNATE PATH CWE-424

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.

CVE-2022-1742 has been assigned to this vulnerability.

2.2.5 PATH TRAVERSAL: '../FILEDIR' CWE-24

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.

CVE-2022-1743 has been assigned to this vulnerability.

2.2.6 EXECUTION WITH UNNECESSARY PRIVILEGES CWE-250

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.

CVE-2022-1744 has been assigned to this vulnerability.

2.2.7 AUTHENTICATION BYPASS BY SPOOFING CWE-290

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.

CVE-2022-1745 has been assigned to this vulnerability.

2.2.8 INCORRECT PRIVILEGE ASSIGNMENT CWE-266

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.

CVE-2022-1746 has been assigned to this vulnerability.

2.2.9 ORIGIN VALIDATION ERROR CWE-346

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.

CVE-2022-1747 has been assigned to this vulnerability.

Watch:

CISA claimed: ‘’CISA has no evidence that these vulnerabilities have been exploited in any elections.’’ We can conclude that they could have been used in the 2020 election.

The report added: ‘’Exploitation of these vulnerabilities would require physical access to individual ImageCast X devices, access to the Election Management System (EMS), or the ability to modify files before they are uploaded to ImageCast X devices.’’

Category

1. Crime-Justice-Terrorism-Corruption
2. Main
3. Politics-Geopolitics-Gov.-Events

Date Created
06/08/2022