



CVE-2022-1742

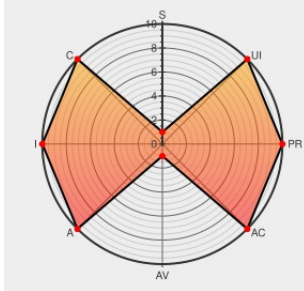
Published on: Not Yet Published

Last Modified on: 07/06/2022 02:10:00 AM UTC

CVE-2022-1742 - advisory for

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Democracy Suite](#) from [Dominionvoting](#) contain the following vulnerability:

The tested version of Dominion Voting Systems 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 by [@ics-cert@hq.dhs.gov](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Dominion Voting Systems](#) - **ImageCast X application** version **None Versions 5.5.10.30 and 5.5.10.32**

Affected Vendor/Software: [Dominion Voting Systems](#) - **ImageCast X firmware** version **None Version 5.5-A**

CVSS3 Score: **6.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Taas	Link
-------------	------	------

Vulnerabilities Affecting Dominion Voting Systems ImageCast X | CISA

[www.cisa.gov](https://www.cisa.gov/text/html)
text/html

MISC www.cisa.gov/uscert/ics/advisories/icsa-22-154-01

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Dominionvoting	Democracy Suite	5.5-a	All	All	All
Application	Dominionvoting	Imagecast X	5.5.10.30	All	All	All
Application	Dominionvoting	Imagecast X	5.5.10.32	All	All	All
Operating System	Dominionvoting	Imagecast X	All	All	All	All
cpe:2.3:h:dominionvoting:democracy_suite:5.5-a:*:*:*:*:*:						
cpe:2.3:a:dominionvoting:imagecast_x:5.5.10.30:*:*:*:*:*:						
cpe:2.3:a:dominionvoting:imagecast_x:5.5.10.32:*:*:*:*:*:						
cpe:2.3:o:dominionvoting:imagecast_x:*:*:*:*:*:						

Social Mentions

Source	Title	Posted (UTC)
 @RedPacketSec	Dominion Voting Systems ImageCast X privilege escalation CVE-2022-1742 - redpacketsecurity.com/dominion-votin...	2022-06-04 09:01:36
 @threatmeter	CVE-2022-1742 Dominion Democracy Suite Voting System 5.5-A ImageCast X access control (icsa-22-154-01) A vulnerab... twitter.com/i/web/status/1...	2022-06-06 07:50:41
 @CVEreport	CVE-2022-1742 : The tested version of Dominion Voting Systems ImageCast X allows for rebooting into Android Safe Mo... twitter.com/i/web/status/1...	2022-06-24 15:13:44

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)

