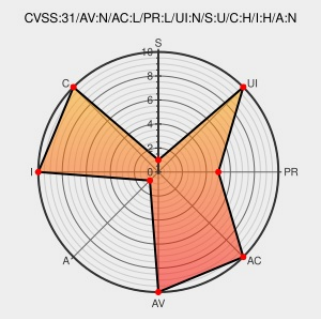
CVE-2020-11681

Published on: 06/04/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:25 PM UTC

CVE-2020-11681

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nextgen Dvr from Castel contain the following vulnerability:

Castel NextGen DVR v1.0.0 stores and displays credentials for the associated SMTP server in cleartext. Low privileged users can exploit this to create an administrator user and obtain the SMTP credentials.

CVE-2020-11681 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Castel NextGen DVR 1.0.0 Bypass / CSRF / Disclosure ≈ Packet Storm	Third Party Advisory, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/157954/Castel-NextGen-DVR-1.0.0-Bypass-CSRF-Disclosure.html
Full Disclosure: Castel NextGen DVR multiple CVEs	Mailing List	FULLDISC 20200605 Castel NextGen DVR multiple

	Third Party Advisory seclists.org text/html	CVEs
Authorization Bypass: A Cautionary Tale CVE (2020-11679, 2020-11680, 2020-11681)	Third Party Advisory www.securitymetrics.com text/html	SM MISC www.securitymetrics.com/blog/attackers-known-unknown-authorization-bypass

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	Castel	Nextgen Dvr	-	All	All	All
Hardware	Castel	Nextgen Dvr	-	All	All	All
Operating System	Castel	Nextgen Dvr Firmware	1.0.0	All	All	All
Operating System	Castel	Nextgen Dvr Firmware	1.0.0	All	All	All

cpe:2.3:h:castel:nextgen_dvr:-:*:*:*:*:*:*:*:

cpe:2.3:h:castel:nextgen_dvr:-:*:*:*:*:*:*:*:

cpe:2.3:o:castel:nextgen_dvr_firmware:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:castel:nextgen_dvr_firmware:1.0.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→