CVE-2020-11679

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-11679
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-04 19:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	Castel NextGen DVR v1.0.0 is vulnerable to privilege escalation through the Adminstrator/Users/Edit/:UserId functionality. A

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Castel NextGen DVR 1.0.0 Bypass / CSRF / Disclosure ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Th
Full Disclosure: Castel NextGen DVR multiple CVEs	FULLDISC	seclists.org	Exploit, Ma
Authorization Bypass: A Cautionary Tale CVE (2020-11679, 2020-11680, 2020-11681)	MISC	www.securitymetrics.com	Exploit, Th
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report