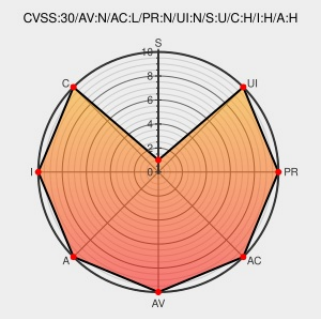
CVE-2018-9995

Published on: 04/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:54 PM UTC

CVE-2018-9995

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



Certain versions of Tbk-dvr4104 from Tbkvision contain the following vulnerability:

TBK DVR4104 and DVR4216 devices, as well as Novo, CeNova, QSee, Pulnix, XVR 5 in 1, Securus, Night OWL, DVR Login, HVR Login, and MDVR Login, which run re-branded versions of the original TBK DVR4104 and DVR4216 series, allow remote attackers to bypass authentication via a "Cookie: uid=admin" header, as demonstrated by a device.rsp?opt=user&cmd=list request that provides credentials within JSON data in a response.

CVE-2018-9995 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Capitan Alfa: [TBK Vision] DVR Login Bypass	Exploit	MISC misteralfa.hack.blogspot.cl/2018/04/tbk-vision-dvr...

Capitan Alfa: [TBK Vision] DVR Login Bypass (CVE-2018-9995)	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC misteralfa-hack.blogspot.cl/2018/04/tbk-vision-dvr-login-bypass.html
TBK DVR4104 / DVR4216 - Credentials Leak - Hardware remote Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 44577
New Hacking Tool Lets Users Access a Bunch of DVRs and Their Video Feeds	Exploit Third Party Advisory www.bleepingcomputer.com text/html	MISC www.bleepingcomputer.com/news/security/new-hacking-tool-lets-users-access-a-bunch-of-dvrs-and-their-video-feeds/
Capitan Alfa: [update] DVR Login Bypass (CVE-2018-9995)	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC misteralfa-hack.blogspot.cl/2018/04/update-dvr-login-bypass-cve-2018-9995.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tbkvision	Tbk-dvr4104	-	All	All	All
Hardware	Tbkvision	Tbk-dvr4104	-	All	All	All
Operating System	Tbkvision	Tbk-dvr4104 Firmware	-	All	All	All
Operating System	Tbkvision	Tbk-dvr4104 Firmware	-	All	All	All
Hardware	Tbkvision	Tbk-dvr4216	-	All	All	All
Hardware	Tbkvision	Tbk-dvr4216	-	All	All	All
Operating System	Tbkvision	Tbk-dvr4216 Firmware	-	All	All	All
Operating System	Tbkvision	Tbk-dvr4216 Firmware	-	All	All	All

cpe:2.3:h:tbkvision:tbk-dvr4104:-:*:*:*:*:*:*:*:

cpe:2.3:h:tbkvision:tbk-dvr4104:-:*:*:*:*:*:*:*:

cpe:2.3:o:tbkvision:tbk-dvr4104_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:tbkvision:tbk-dvr4104_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:tbkvision:tbk-dvr4216:-:*:*:*:*:*:*:*:

cpe:2.3:h:tbkvision:tbk-dvr4216:-:*:*:*:*:*:*:*:

cpe:2.3:o:tbkvision:tbk-dvr4216_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:tbkvision:tbk-dvr4216_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEtrends	Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2023-0266: 370.6K (audience size) CVE-2018-9995: 343.7K CVE-2016-2… twitter.com/i/web/status/1…	2023-05-04 13:00:04
/r/PFSENSE	help: Suricata shuts down after several minutes	2022-04-09 16:21:29

← Previous ID

Next ID→