CVE-2021-42109

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

Summary

CVE	CVE-2021-42109
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-08 18:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	VITEC Exterity IPTV products through 2021-04-30 allow privilege escalation to root.

Risk And Classification

Problem Types: CWE-1188

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Vitec	Avediastream M9305	-	All	All	All
Operating System	Vitec	Avediastream M9305 Firmware	All	All	All	All
Hardware	Vitec	Avediastream M9325	-	All	All	All
Operating System	Vitec	Avediastream M9325 Firmware	All	All	All	All
Hardware	Vitec	Avediastream M9400	-	All	All	All
Operating System	Vitec	Avediastream M9400 Firmware	All	All	All	All
Hardware	Vitec	Avediastream M9405	-	All	All	All
Operating System	Vitec	Avediastream M9405 Firmware	All	All	All	All
Hardware	Vitec	Avediastream M9605	-	All	All	All
Operating System	Vitec	Avediastream M9605 Firmware	All	All	All	All
Hardware	Vitec	Avediastream R9300	-	All	All	All
Operating System	Vitec	Avediastream R9300 Firmware	All	All	All	All
Hardware	Vitec	Avediastream R9310	-	All	All	All
Operating System	Vitec	Avediastream R9310 Firmware	All	All	All	All
Hardware	Vitec	Avediastream R9350	-	All	All	All
Operating System	Vitec	Avediastream R9350 Firmware	All	All	All	All
Application	Vitec	Exterity Avediaserver	All	All	All	All

Hardware	Vitec	Exterity Avediastream Encoders	-	All	All	All
Operating System	Vitec	Exterity Avediastream Encoders Firmware	All	All	All	All

References

Reference	Source	Link	Tags
IoT Hacking and Rickrolling My High School District | WhiteHoodHacker	MISC	whitehoodhacker.net	
IPTV Technology and Digital Signage Solutions I Exterity	MISC	www.exterity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |
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 registred 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.

Free CVE JSON API cve.report/api

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