CVE-2022-36159

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

Summary

CVE	CVE-2022-36159
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-26 11:15:00 UTC
Updated	2022-10-03 17:16:00 UTC
Description	Contec FXA3200 version 1.13 and under were discovered to contain a hard coded hash password for root stored in the cor

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Contec	Fxa2000	-	All	All	All
Operating System	Contec	Fxa2000 Firmware	All	All	All	All
Hardware	Contec	Fxa3000	-	All	All	All
Operating System	Contec	Fxa3000 Firmware	All	All	All	All
Hardware	Contec	Fxa3020	-	All	All	All
Operating System	Contec	Fxa3020 Firmware	All	All	All	All
Hardware	Contec	Fxa3200	-	All	All	All
Operating System	Contec	Fxa3200 Firmware	All	All	All	All

References

Reference	Source	Link
gist.github.com/Nwqda/aac33d1936d2b514a3268f145345abb4	MISC	gist.gi
JVNVU#98305100: Multiple vulnerabilities in Contec FLEXLAN FX3000 and FX2000 series	MISC	jvn.jp
Contec FLEXLAN FXA2000 and FXA3000 series vulnerability report - Necrum Security Labs	MISC	samy.
Overview / Features | FXA3200 | Simultaneous connection type Wireless LAN Access Point (Master Station) | CONTEC	MISC	www.c
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

591367 Contec FLEXLAN FX3000 and FX2000 series Hidden Functionality and Use of Hard-coded Credentials Multiple Vulnerabilities (JVNVU98305100)

Free CVE JSON API cve.report/api

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