FXC AE1021, AE1021PE OS Command Injection Vulnerability

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

Summary

CVE	CVE-2023-49897
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-06 07:15:00 UTC
Updated	2023-12-06 13:50:00 UTC
Description	FXC AE1021 and AE1021PE contain an OS command injection vulnerability that allows authenticated users to execute cor

Risk And Classification

EPSS: 0.244130000 probability, percentile 0.961480000 (date 2026-05-10)

CISA KEV: Listed on 2023-12-21; due 2024-01-11; ransomware use Unknown

CISA Known Exploited Vulnerability

Vendor	FXC
Product	AE1021, AE1021PE
Name	FXC AE1021, AE1021PE OS Command Injection Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://www.fxc.jp/news/20231206 ; https://nvd.nist.gov/vuln/detail/CVE-2023-49897

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link
AE1021/AE1021PEのファームウェア Ver2.0.10 公開のお知らせ		www.fxc.jp
JVNVU#92152057: FXC wireless LAN routers "AE1021PE" and "AE1021" vulnerable to OS command injection		jvn.jp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

62085 For Vulnerability CVE-2023-49897

731363 For Vulnerability CVE-2023-49897

Free CVE JSON API cve.report/api

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