



CVE-2023-39429

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-39429
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-03 01:15:00 UTC
Updated	2023-10-04 17:08:00 UTC
Description	Cross-site scripting vulnerability in FURUNO SYSTEMS wireless LAN access point devices allows an authenticated user to

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Furunosystems	Acera 1010	-	All	All	All
Operating System	Furunosystems	Acera 1010 Firmware	All	All	All	All
Hardware	Furunosystems	Acera 1020	-	All	All	All
Operating System	Furunosystems	Acera 1020 Firmware	All	All	All	All
Hardware	Furunosystems	Acera 1110	-	All	All	All
Operating System	Furunosystems	Acera 1110 Firmware	All	All	All	All
Hardware	Furunosystems	Acera 1150i	-	All	All	All
Operating System	Furunosystems	Acera 1150i Firmware	All	All	All	All
Hardware	Furunosystems	Acera 1150w	-	All	All	All
Operating System	Furunosystems	Acera 1150w Firmware	All	All	All	All
Hardware	Furunosystems	Acera 1210	-	All	All	All
Operating System	Furunosystems	Acera 1210 Firmware	All	All	All	All
Hardware	Furunosystems	Acera 800st	-	All	All	All
Operating System	Furunosystems	Acera 800st Firmware	All	All	All	All
Hardware	Furunosystems	Acera 810	-	All	All	All
Operating System	Furunosystems	Acera 810 Firmware	All	All	All	All
Hardware	Furunosystems	Acera 850f	-	All	All	All

Operating System	Furunosystems	Acera 850f Firmware	All	All	All	All
Hardware	Furunosystems	Acera 850m	-	All	All	All
Operating System	Furunosystems	Acera 850m Firmware	All	All	All	All
Hardware	Furunosystems	Acera 900	-	All	All	All
Operating System	Furunosystems	Acera 900 Firmware	All	All	All	All
Hardware	Furunosystems	Acera 950	-	All	All	All
Operating System	Furunosystems	Acera 950 Firmware	All	All	All	All

References

Reference	Solution
JVNVU#94497038: Multiple vulnerabilities in multiple FURUNO SYSTEMS wireless LAN access point devices in ST(Standalone) mode	MIS
【重要】無線LANアクセスポイント「STモード」における複数の脆弱性と対処方法について 業務用wifi(無線lan)のフルノシステムズ	MIS
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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