CVE-2020-21884

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

Summary

CVE	CVE-2020-21884
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-09 13:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	Unibox SMB 2.4 and UniBox Enterprise Series 2.4 and UniBox Campus Series 2.4 contain a cross-site request forgery (CS

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Indionetworks	Unibox U1000	-	All	All	All
Operating System	Indionetworks	Unibox U1000 Firmware	2.4	All	All	All
Hardware	Indionetworks	Unibox U2500	-	All	All	All
Operating System	Indionetworks	Unibox U2500 Firmware	2.4	All	All	All
Hardware	Indionetworks	Unibox U50	-	All	All	All
Hardware	Indionetworks	Unibox U500	-	All	All	All
Hardware	Indionetworks	Unibox U5000	-	All	All	All
Operating System	Indionetworks	Unibox U5000 Firmware	2.4	All	All	All
Operating System	Indionetworks	Unibox U500 Firmware	2.4	All	All	All
Operating System	Indionetworks	Unibox U50 Firmware	2.4	All	All	All

References

Reference	Source	Link
[FD] KSA-Dev-008: Authenticated XSRF leads to complete account takeover in all UNIBOX WiFi Hotspot Controller		www.mail-
s3curityb3ast.github.io/KSA-Dev-008.txt	MISC	s3curityb3
Wifisoft - Enterprise WiFi, WiFi Hotspots and IOT Solutions	MISC	wifi-soft.cc
[FD] KSA-Dev-008: Authenticated XSRF leads to complete account takeover in all UNIBOX WiFi Hotspot Controller	MISC	www.mail-

CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

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