CVE-2020-36056

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

Summary

CVE	CVE-2020-36056
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-31 13:15:00 UTC
Updated	2022-09-30 14:49:00 UTC
Description	Beetel 777VR1-DI Hardware Version REV.1.01 Firmware Version V01.00.09_55 was discovered to contain a cross-site scr

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Beetel	777vr1	1.01	All	All	All
Hardware	Beetel	777vr1-dl	1.01	All	All	All
Operating System	Beetel	777vr1-dl Firmware	01.00.09_55	All	All	All
Operating System	Beetel	777vr1 Firmware	01.00.09_55	All	All	All

References

Reference
CVE-2020-36056 beetel Moderm 777vr1 — Cross Site Scripting on the beetel 777vr1 via the Ping Diagnostic · Issue #5 · VivekPanday12/CVE
www.linkedin.com/in/vivek-panday-796768149
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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