CVE-2020-25755

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

Summary

CVE	CVE-2020-25755
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-16 19:15:00 UTC
Updated	2022-05-03 16:04:00 UTC
Description	An issue was discovered on Enphase Envoy R3.x and D4.x (and other current) devices. The upgrade_start function in /insta

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Enphase	Envoy	-	All	All	All
Operating System	Enphase	Envoy Firmware	d4.0	All	All	All
Operating System	Enphase	Envoy Firmware	r3.0	All	All	All

References

Reference	Source
Can solar controllers be used to generate fake clean energy credits? | by Waylon Grange | Stage 2 Security | May, 2021 | Medium	MISC
Cloud Native Cyber Security | Stage 2 Security | United States	MISC
Enphase Envoy: Gateway to a Connected Smart Home | Enphase	MISC
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

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