CVE-2020-35579

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

Summary

CVE	CVE-2020-35579
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-20 07:15:00 UTC
Updated	2020-12-22 19:49:00 UTC
Description	tindy2013 subconverter 0.6.4 has a /sub?target=%TARGET%&url=%URL%&config=%CONFIG% API endpoint that accepts

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Subconverter Project	Subconverter	0.6.4	All	All	All
Application	Subconverter Project	Subconverter	0.6.4	All	All	All

References

Reference
[vulnerability] Loop Request检测存在问题，可实现拒绝服务攻击 / Loop Request detection is too fragile and can realize denial of service attack
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**