CVE-2021-42750

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

Summary

CVE	CVE-2021-42750
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-12 17:15:00 UTC
Updated	2022-08-15 19:04:00 UTC
Description	A cross-site scripting (XSS) vulnerability in Rule Engine in ThingsBoard 3.3.1 allows remote attackers (with administrative a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Thingsboard	Thingsboard	3.3.1	All	All	All

References

Reference	Source
Thingsboard 3.3.1 Cross Site Scripting ≈ Packet Storm	MISC
GitHub - thingsboard/thingsboard: Open-source IoT Platform - Device management, data collection, processing and visualization.	MISC
CVE Program record	CVE.ORG
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**