CVE-2022-45608

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

Summary

CVE	CVE-2022-45608
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-01 16:15:00 UTC
Updated	2023-05-11 16:15:00 UTC
Description	An issue was discovered in ThingsBoard 3.4.1, allows low privileged attackers (CUSTOMER_USER) to gain escalated privi

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Thingsboard	Thingsboard	3.4.1	All	All	All

References

Reference	Source	Link
Responsible disclosure: Access control vulnerability discovered in the ThingsBoard IoT platform | Outpost24 blog	MISC	outpost24.co
thingsboard.com	MISC	thingsboard.(
(CVE-2022-45608) ThingsBoard Access Control Privilege Escalation | DELLOS | Offensive Blog	MISC	wiki.wizard32
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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