



# CVE-2021-42750

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-42750
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-12 17:15:00 UTC
<b>Updated</b>	2022-08-15 19:04:00 UTC
<b>Description</b>	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.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)