



CVE-2022-23126

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-23126
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-24 19:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	TeslaMate before 1.25.1 (when using the default Docker configuration) allows attackers to open doors of Tesla vehicles, st

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Teslamate Project	Teslamate	All	All	All	All

References

Reference
Release v1.25.1 · adriankumpf/teslamate · GitHub
Teslascope on Twitter: "Just to chime in, any vehicles on TezLab were not at any risk of "full remote control" and as such, vehicles whether on
How I got access to 25+ Tesla's around the world. By accident. And curiosity. by David Colombo Jan, 2022 Medium
How I got access to 25+ Tesla's around the world. By accident. And curiosity. by David Colombo Medium
Comparing v1.25.0...v1.25.1 · adriankumpf/teslamate · GitHub
Disable anonymous login to Grafana · adriankumpf/teslamate@fff6915 · GitHub
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)