



traccar allows XML injection in KML and GPX exports

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

Summary

CVE	CVE-2026-27693
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-05 13:16:28 UTC
Updated	2026-05-08 20:04:19 UTC
Description	Traccar is an open source GPS tracking system. In org.traccar:traccar versions starting at 6.11.1 before 6.13.0, the KML ar

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from security-advisories@github.com

CVSS: 3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:L

EPSS: 0.000430000 probability, percentile 0.129980000 (date 2026-05-12)

Problem Types: CWE-91 | CWE-91 CWE-91: XML Injection (aka Blind XPath Injection)

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:L
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

None

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:L

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Traccar	Traccar	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Traccar	Traccar	affected >= 6.11.1, < 6.13.0	Not specified

References

Reference	Source	Link	Tags
github.com/traccar/traccar/blob/v6.11.0/src/main/java/org/traccar/report...	security-advisories@github.com	github.com	Produ...
github.com/traccar/traccar/security/advisories/GHSA-32pj-vrqq-x656	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploi...
CVE Program record	CVE.ORG	www.cve.org	canoni...
NVD vulnerability detail	NVD	nvd.nist.gov	canoni...

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](#)