contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

TPC Software Matchpoint: new CVE

CVE-2026-111489 · record published 5 November 2026

Analysis Report

Anyone running TPC Software Matchpoint should update the mobile app to the latest available version as soon as possible; the record scores this 9.9 out of 10. Contact TPC Software to obtain the ...

PREPARED BY	NamiQ	DATE	6 November 2026
FACTS AS OF	6 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 9.9**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/tpc-software-matchpoint-cve-2026-111489

The bottom line

> *Anyone running TPC Software Matchpoint should update the mobile app to the latest available version as soon as possible; the record scores this 9.9 out of 10. Contact TPC Software to obtain the current release and confirm the server-side fixes are in place.*

At a glance

Fact	Detail
Product	TPC Software Matchpoint (CVE-2026-111489)
Severity	Critical: 9.9 (CVSS 4.0)
Status	A new CVE record, published by INCIBE on 5 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 6 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	The vendor statement in the record recommends installing 'the latest available version' but does not name a version number.
Who looks first	Organisations that have deployed the TPC Software Matchpoint mobile app to staff or customers. The record does not restrict the exposure to a particular network zone.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run TPC Software Matchpoint?	Nothing to do for this CVE.	Check whether the mobile app is deployed to any users.
Is the Matchpoint mobile app deployed to staff or customers?	Review the server-side guidance; monitor for further vendor advice.	Find out which app version is installed and move to update.
Can untrusted parties reach the Matchpoint API over the network?	Patch within your normal cycle.	Treat as urgent and update the app to the latest version promptly.

What it is

A credential hard-coded into the Matchpoint mobile app can be presented to the platform to receive the 'autorizado' authentication token without supplying any user password. The record states this

grants unauthenticated access to API services.

Why it matters

A score of 9.9 reflects that no login is required: the credential is in the app itself, so anyone who can reach the API may use it. Our reading is that exposure is highest where the API faces the internet or an untrusted network, because there is no authentication barrier to overcome. The vendor statement in the record notes that server-side fixes for CVE-2026-111490 and CVE-2026-111493 are already deployed regardless of app version; this CVE requires an app update to resolve.

Things people will get wrong

- The server patch already deployed covers this CVE The vendor statement in the record is explicit: the deployed server fixes cover CVE-2026-111490 and CVE-2026-111493 only. This CVE requires the latest app version to be installed.
- Only a specific version is affected; an older release may be safe The record lists all versions prior to the latest as affected. No safe older version is named.

How we would triage it

This is our judgement.

Step 1: Find the Matchpoint app version in use

- Ask your Matchpoint administrator or TPC Software which version of the mobile app is currently deployed to users.
- Confirm whether the Matchpoint server-side updates are in place; the vendor statement in the record says fixes for CVE-2026-111490 and CVE-2026-111493 are deployed automatically.

Step 2: Restrict API access while you arrange the update

- If the Matchpoint API is reachable from outside the organisation, consider restricting access to trusted IP ranges until the app is updated.
- The record does not describe a workaround; network restriction is a temporary measure only.

Step 3: Update the mobile app to the latest available version

- The vendor statement in the record recommends installing the latest available version; contact TPC Software for the current release number.
- The record does not name the fixed version, so written confirmation from TPC Software of the version that addresses this CVE is advisable.

Step 4: Confirm the fix and document it

- Obtain written confirmation from TPC Software or your Matchpoint administrator that the latest app version is installed and that CVE-2026-111489 is addressed.
- Record the version number and the confirmation date for your audit trail.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are reviewing CVE-2026-111489, a recently published vulnerability in TPC Software Matchpoint scored 9.9 out of 10. A static credential in the mobile app can be used to obtain an authentication token without a password, granting access to API services. The CVE record states that server-side fixes for two related issues (CVE-2026-111490 and CVE-2026-111493) are already deployed, but installing the latest app version is required to address this CVE. Please confirm whether we run Matchpoint, which version of the app is installed, whether the server-side fixes are confirmed in place, and when the app can be updated to the latest version. We would like written confirmation of the installed version and the fix by [date].*

The sources, in their words

The CVE record:

> *A static credential embedded in the mobile app has been reported to return the 'autorizado' token on the MatchPoint platform. The report states that this token grants unauthenticated access to API services.*

Versions of TPC Software Matchpoint the record lists as affected:

- Versions prior to latest one

The record gives no version ranges. Use the vendor's advisory for the affected versions.

What the record says to do about it, in the vendor's words:

> *The manufacturer has announced the following measures. The server fixes for CVE-2026-111490 and CVE-2026-111493 have already been deployed and are applied regardless of the app version. To address the remaining vulnerabilities, it is recommended that you install the latest available version.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-111489
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-111489
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. It reads the names of the running images, not what is inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The record does not name the fixed version number; the vendor says 'latest available version' without specifying it.
- The record does not say which API services or data are accessible using the token obtained with the static credential.
- The record does not describe how easily the static credential can be extracted from the app binary.
- The scores and details for CVE-2026-111490 and CVE-2026-111493, referenced in the vendor statement, are not included in this record.
- Exploitation is not recorded. That is not the same as none.

- This is a new record: scores, versions and wording can change in the first days, and they are as at 6 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-111489: score 9.9, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	None	No effect on availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
5 November 2026	CVE record published by INCIBE.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Matchpoint mobile app deployed and the API is reachable from outside the organisation	High	Update the app immediately

Matchpoint mobile app deployed and the API is on an internal network only	High	Update the app this week
Matchpoint server in use but the mobile app has not been deployed to users	Medium	Confirm server-side fixes; monitor for vendor guidance
TPC Software Matchpoint is not in use	None	No action needed for this CVE

Appendix 4. Definition of done

- Every TPC Software Matchpoint you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-111489: https://www.cve.org/CVERecord?id=CVE-2026-111489
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: www.incibe.es: https://www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-tpc-softwares-matchpoint