contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center: new CVE

CVE-2026-14914 · record published 20 November 2026

Analysis Report

Anyone running Tegsoft Contact Center must act immediately — the record assigns a CVSS score of 10, the maximum. First, confirm whether this product is deployed in

PREPARED BY	NamiQ	DATE	21 November 2026
FACTS AS OF	21 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 10.0**	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/tegsoft-yo-netim-ve-bilis-im-hizmetleri-tic-cve-2026-14914

The bottom line

> *Anyone running Tegsoft Contact Center must act immediately — the record assigns a CVSS score of 10, the maximum. First, confirm whether this product is deployed in your estate; if it is, update to latest-202611161510 without delay.*

At a glance

Fact	Detail
Product	Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center (CVE-2026-14914)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by TR-CERT on 20 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 21 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	The record states all versions before latest-202611161510 are affected, making that the first unaffected version. No vendor advisory was available to confirm this.
Who looks first	Any organisation running Tegsoft Contact Center on a version before latest-202611161510, particularly where the application is reachable from the internet or from users who are not fully trusted.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Tegsoft Contact Center anywhere in your estate?	Nothing to do for this CVE.	Check the installed version (next question).
Is your installed version before latest-202611161510?	You are on the unaffected version; monitor for further guidance.	Update immediately; your version is affected.
Is the application reachable from the internet or from untrusted users?	Restrict access and update at the next available opportunity.	Treat this as urgent; update and restrict upload access in parallel.

What it is

An attacker can upload a file of any type — including a web shell — to the server. Once on the server, that file can be used to run commands as if the attacker were inside it. The record names CWE-434:

unrestricted upload of a file with a dangerous type.

Things people will get wrong

- It is not on CISA's exploited list, so it can wait. The record was published 20 November 2026; absence from the exploited list reflects how new it is. A CVSS score of 10 is the highest severity regardless of confirmed exploitation.
- Only users who already have upload access are a risk. The record does not say whether the upload endpoint requires authentication. A score of 10 suggests it may not; treating it as unauthenticated is the safer assumption until the vendor clarifies.

How we would triage it

This is our judgement.

Step 1: Find which version of Tegsoft Contact Center you run

- Check the application's admin or settings panel for a build or version string.
- Compare it against latest-202611161510; the record says any earlier version is affected.

Step 2: Restrict access to file upload while preparing the update

- If the admin panel allows the upload feature to be disabled, disable it temporarily.
- If the application is internet-facing, consider restricting network access to it until the update is applied.

Step 3: Update to latest-202611161510 or later

- Apply the update using the vendor's standard update mechanism.
- The record names latest-202611161510 as the first unaffected version; confirm the version string after updating.

Step 4: Confirm the update and restore normal access

- Verify the version string shows latest-202611161510 or later before restoring access.
- Record the version and the date of the update for your change log.

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 have been made aware of a security flaw in Tegsoft Contact Center, CVE-2026-14914, with a CVSS score of 10. The record was published 20 November 2026. The flaw allows an attacker to upload a web shell and run commands on the server. The record lists all versions before latest-202611161510 as affected. Please confirm whether we run this product, which version is installed, and whether it is reachable from the internet. If we are on an affected version, please advise on the steps to update to latest-202611161510 and provide written confirmation of the installed version and the date the update is applied.*

The weakness behind it

The record classes this as CWE-434.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in a web application; an external attacker would likely exploit the upload endpoint over the internet, fitting exploitation of a public-facing application.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	Uploading a web shell is the named exploitation path; a web shell would execute attacker-supplied commands on the server via a scripting interpreter.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *Unrestricted upload of file with dangerous type vulnerability in Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center allows Upload a Web Shell to a Web Server. This issue affects Tegsoft Contact Center: before latest-202611161510.*

Versions of Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center the record lists as affected:

- all versions before latest-202611161510

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

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-2026-14914
```

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 hardware (maker, model, firmware), the running container images with their operating system and packages, 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-2026-14914
```

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. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages 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

- Whether authentication is required to reach the file upload endpoint — the record does not say.
- Which specific endpoint or feature within the application is affected.
- Whether the update to latest-202611161510 is applied automatically or requires a manual administrator action.
- 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 21 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", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "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-2026-14914: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` 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.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
20 November 2026	CVE record published by TR-CERT.

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
Tegsoft Contact Center deployed and directly reachable from the internet	Medium	immediately
Tegsoft Contact Center deployed on an internal network only, affected version	Medium	this week
Tegsoft Contact Center deployed; file upload restricted by a network or WAF rule	Medium	this week — a firewall rule is not a fix
Not running Tegsoft Contact Center	None	none for this CVE

Appendix 4. Definition of done

- Every Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center 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-2026-14914: https://www.cve.org/CVERecord?id=CVE-2026-14914
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: siberguvenlik.gov.tr: https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-1588