contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Openwave Messaging Limited Webtop Media Transcoder exploited

CVE-2026-111793 · on CISA's exploited list since 10 November 2026

Analysis Report

Organisations running Webtop Media Transcoder before version 1.1.22.0 must apply the vendor patch by 24 November 2026. Contact Openwave Messaging now to

PREPARED BY	NamiQ	DATE	11 November 2026
FACTS AS OF	11 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 3.1 4.3**	STATUS	On CISA's exploited list; due 24 November 2026

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/openwave-messaging-limited-webtop-media-cve-2026-111793

The bottom line

> *Organisations running Webtop Media Transcoder before version 1.1.22.0 must apply the vendor patch by 24 November 2026. Contact Openwave Messaging now to obtain it.*

At a glance

Fact	Detail
Product	Openwave Messaging Limited Webtop Media Transcoder (CVE-2026-111793)
Severity	Medium: 4.3 (CVSS 3.1)
CISA	On its exploited list since 10 November 2026. Deadline for US federal agencies: 24 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 11 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	The JVN advisory lists all versions before 1.1.22.0 as affected; 1.1.22.0 is the first version not listed as affected. Contact Openwave to obtain the patch — the advisory gives no further procedural details.
Who looks first	Anyone running Webtop Media Transcoder (Openwave Messaging) on a version before 1.1.22.0, particularly where authenticated users can reach the transcoder directly rather than only through the standard Webmail interface.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you use Webtop Media Transcoder, supplied by Openwave Messaging?	Nothing to do for this CVE.	Find the installed version.
Is the installed version earlier than 1.1.22.0?	Not in the affected range; monitor for further vendor advisories.	Contact Openwave for the patch immediately.
Can authenticated users reach the transcoder directly, bypassing the Webmail interface?	Exposure is reduced; patch when the vendor provides it.	Prioritise patching before 24 November 2026.

What it is

An authenticated user can upload a specially crafted file to bypass the administrator-set file-type restrictions in the transcoder. The JVN advisory says this may allow that user to obtain sensitive information the system holds.

Why it matters

The CVSS score is 4.3, but the JVN advisory states that attacks exploiting this vulnerability have been observed. The flaw bypasses administrator-set file-type controls in the transcoder. Our reading is that the most likely use is by an authenticated account reaching the transcoder directly — outside the Webmail path — to submit a crafted file and read back content that should have been refused. The risk is information disclosure from within the platform, not remote unauthenticated access.

What the vendor's advisory says

We read one page on jvn.jp. In short:

- The JVN advisory (published 9 November 2026) states that a patch exists and instructs contacting Openwave for details. No other vulnerabilities are described in the same release, and no workaround is listed.

Things people will get wrong

- The score is only 4.3, so this is not urgent. The JVN advisory states attacks exploiting this have been observed, and CISA has set a deadline of 24 November 2026. Score alone does not reflect exploitation activity.
- Only external attackers are a concern here. The flaw requires authentication. An insider or a compromised credential is the more likely path, since an external attacker would first need to obtain a valid account.

The wording includes conditions the score may not show: the attacker must be logged in. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the version you run

- Log in to the Webtop Media Transcoder admin interface and check the version number displayed.

- Compare it against the affected range: the JVN advisory lists all versions before 1.1.22.0 as affected.

Step 2: Restrict direct transcoder access while awaiting the patch

- Limit which authenticated users can reach the transcoder API directly, keeping access to only those whose role requires it.
- Ensure other users can only access transcoder functions through the standard Webmail path, which the record identifies as the intended route.

Step 3: Obtain and apply the patch

- Contact Openwave Messaging directly to request the patch, as instructed by the JVN advisory.
- Apply the patch according to the vendor's instructions; the advisory does not give further procedural detail.

Step 4: Review transcoder logs if the product was exposed

- Check transcoder access logs for requests involving file types outside the administrator-defined allowed list.
- Look for requests that arrived outside the standard Webmail path, which the record identifies as the bypass route.

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. CISA's wording adds that you should stop using the product if no mitigation is available.

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 notified of CVE-2026-111793, which affects Webtop Media Transcoder (Openwave Messaging) in all versions before 1.1.22.0. The flaw allows an authenticated user to bypass file-type restrictions in the transcoder and may allow sensitive information to be obtained. CISA has set a remediation deadline of 24 November 2026. Please can you confirm: (1) whether we run Webtop Media Transcoder, and if so which version; (2) whether the patch from Openwave has been obtained and applied; and (3) whether any authenticated user can access the transcoder directly outside the standard Webmail interface. We would like written confirmation of the installed version and fix status by 21 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Transcoder access logs showing submissions of file types outside the administrator-defined allowed list.
- Requests to the transcoder that did not originate through the standard Webmail interface, which is identified in the record as the bypass route.

The weakness behind it

The record classes this as CWE-669 (Incorrect Resource Transfer Between Spheres).

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
Data from Local System (T1005): Copying data stored on the machine.	Collection: gathering data	The flaw may allow an authenticated user to retrieve content by making the transcoder process file types it should refuse, which would likely result in data being read from the local system.
File and Directory Discovery (T1083): Listing files and folders to find what is there.	Discovery: looking around	Bypassing file-type restrictions could allow an authenticated user to probe which file types the transcoder can access, aiding discovery of accessible content on the host.

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

CISA's catalogue entry:

> *Openwave Messaging Limited Webtop Media Transcoder contains an incorrect resource transfer between spheres vulnerability that may allow an authenticated user to process and convert unintended document types if bypassing the Webmail experience.*

The CVE record, published by Mitre on 16 October 2026:

> *Openwave Webtop Media Transcoder does not enforce administrator-defined file type restrictions to restrict the file-types to be converted. This may allow an authenticated user to process and convert unintended document types if bypassing the Webmail experience.*

Versions of Openwave Messaging (Ireland) Limited Webtop Media Transcoder the record lists as affected:

- all versions before 1.1.22.0

The affected ranges end before 1.1.22.0. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

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-2026-111793
```

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-2026-111793
```

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

- The sources do not describe which specific file types can be misused or what categories of sensitive information are at risk.
- No workaround short of patching is described; whether restricting direct API access to the transcoder fully mitigates the flaw is not stated.
- The JVN advisory instructs contacting Openwave for patch details but does not name a release date or distribution channel.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 11 November 2026; the vendor's advisory wins where it differs.
- 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", "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-2026-111793: score 4.3, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

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	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	None	Nothing can be altered.
Availability	Low	Reduced performance or interruptions.

Appendix 2. Timeline

Date	Event
16 October 2026	CVE record published by Mitre.
10 November 2026	CISA added it to its list of exploited vulnerabilities.
24 November 2026	CISA's deadline for US federal agencies.

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
Running Webtop Media Transcoder before version 1.1.22.0 with the transcoder accessible to authenticated users.	High	Before 24 November 2026.
Running the affected version but transcoder access limited to a small set of administrators only.	Medium	This patch cycle.
Webtop Media Transcoder in use but the installed version has not yet been confirmed.	Medium	Determine the version this week.

Webtop Media Transcoder is not installed in this environment.	None	No action needed for this CVE.

Appendix 4. Definition of done

- Every Openwave Messaging Limited Webtop Media Transcoder you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-111793: https://www.cve.org/CVERecord?id=CVE-2026-111793
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: jvn.jp/en/vu/JVNVU93403064/: https://jvn.jp/en/vu/JVNVU93403064/
- Reference in the CVE record: openwave.ai: https://openwave.ai
- Reference in the CVE record: github.com: https://github.com/GISOpenwave/security-advisories-public/blob/main/CAN-2026-2032674.md