contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# open-wanderer wanderer: new CVE

**CVE-2026-71495 · record published 6 November 2026**

## Analysis Report

Anyone running a self-hosted Wanderer instance below 0.20.0 with PUBLIC_PRIVATE_INSTANCE not set to true should update to 0.20.0 now; the fix has been available since 7 July. Start by confirming the …

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 6 November 2026 |
| FACTS AS OF | 6 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/open-wanderer-wanderer-cve-2026-71495

## The bottom line

> *Anyone running a self-hosted Wanderer instance below 0.20.0 with PUBLIC_PRIVATE_INSTANCE not set to true should update to 0.20.0 now; the fix has been available since 7 July. Start by confirming the version and that setting in your docker-compose or environment file.*

## At a glance

| Fact | Detail |
|---|---|
| Product | open-wanderer wanderer (CVE-2026-71495) |
| Severity | Critical: 10 (CVSS 3.1) |
| Status | A new CVE record, published by GitHub on 6 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 | 0.20.0, released 7 July (per the v0.20.0 release notes on GitHub) |
| Who looks first | Anyone operating a self-hosted Wanderer instance below version 0.20.0 where PUBLIC_PRIVATE_INSTANCE is not set to true. No account on the system is needed to trigger the flaw. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run a self-hosted Wanderer instance? | Nothing to do for this CVE. | Check whether your version is below 0.20.0 (next question). |
| Is your Wanderer instance running a version below 0.20.0? | Nothing to do for this CVE. | Check the PUBLIC_PRIVATE_INSTANCE setting (next question). |
| Is PUBLIC_PRIVATE_INSTANCE set to true in your configuration? | The endpoint accepts unauthenticated requests; update to 0.20.0 as soon as possible. | The record says 0.20.0 is the fix; update regardless of this flag. |
| Can anyone outside your organisation reach the Wanderer server? | Risk is lower; still update to 0.20.0 at the next maintenance window. | Update to 0.20.0 as soon as possible; exposure is widest. |

## What it is

The record describes a flaw in the trail download endpoint. An attacker who can reach the server sends a crafted request with any URL in the body; the server fetches it without checking and returns the result. This lets the attacker read from internal services, probe the internal network, or overwhelm internal hosts.

## Why it matters

The record scores this 10 out of 10 under CVSS 3.1, with no authentication required and no user interaction, reachable over the network. The weakness is CWE-918. An attacker who can reach the endpoint directs the server to contact internal services; the record names the database on port 8090, the search service on port 7700, and cloud metadata addresses. Our reading is that reaching cloud metadata is particularly useful for credential theft even without a login to the application. The CVSS scope-change flag reflects that the impact extends beyond the application itself to internal infrastructure.

## What the vendor's advisory says

We read two pages on github.com. In short:

- The v0.20.0 release notes also describe hardened ActivityPub federation and a fix for an N+1 query in follower fanout (PR #1056). No CVE identifier is given for those changes.
- v0.20.0 has breaking changes: integrations now run as sandboxed WASM plugins; trail categories have been reworked. The release notes say operators must update docker-compose.yml for the new /data/plugins folder and install plugins manually after upgrading.

## Things people will get wrong

- Setting PUBLIC_PRIVATE_INSTANCE=true is enough without upgrading. The record identifies 0.20.0 as the fix. The description ties the unauthenticated access to that flag being unset, but the record does not say the flag alone closes the flaw; only 0.20.0 is confirmed.
- Only internet-facing instances are at risk. Any user or system that can reach the Wanderer server can send the crafted request. An internal user or a compromised device on the same network can exploit this without internet access.

## How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

## Step 1: Find the version you run

- Check your docker-compose.yml or the running container image tag for the current version; any version below 0.20.0 is in the affected range.
- If you are unsure which tag is in use, check the compose file for the image line in the wanderer service definition.

```
docker ps --format '{{.Image}}' | grep wanderer
```

## Step 2: Check the PUBLIC_PRIVATE_INSTANCE setting

- Review your environment file or docker-compose.yml for PUBLIC_PRIVATE_INSTANCE; if absent or not set to true, the download endpoint accepts unauthenticated requests and exposure is highest.
- The record names no workaround other than the 0.20.0 update; restricting network access to the server while preparing the update reduces exposure temporarily.

## Step 3: Update to 0.20.0

- Before restarting, update docker-compose.yml to map the new /data/plugins folder in the db service volumes section, as the v0.20.0 release notes require for self-hosted instances.
- Pull the 0.20.0 image, restart the service, and install any plugins following the release notes documentation.

## Step 4: Confirm the update is in place

- After restarting, confirm the running container image is tagged 0.20.0 using the command below.
- Verify that PUBLIC_PRIVATE_INSTANCE is set correctly in the updated configuration.

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 run a self-hosted Wanderer trail database. CVE-2026-71495 describes an unauthenticated server-side request forgery in versions below 0.20.0, which allows anyone who can reach the server to direct it to fetch internal services or cloud metadata addresses. The fix is in version 0.20.0, released 7 July. Could you please confirm: which version of Wanderer we are running; whether PUBLIC_PRIVATE_INSTANCE is set to true in our configuration; and whether the server is reachable from outside our network. If we are below 0.20.0, we would like written confirmation that the update to 0.20.0 has been applied and completed, by [DATE].*

## The weakness behind it

The record classes this as CWE-918.

## 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 network-accessible endpoint requiring no authentication; exploiting it would likely serve as the first step to reach internal infrastructure. |
| Unsecured Credentials: Cloud Instance Metadata API (T1552.005): Reading access tokens from a cloud provider's metadata service. | Credential Access: stealing logins | The record explicitly names cloud metadata addresses as reachable via the SSRF, which would typically serve instance credentials to an attacker. |
| Remote System Discovery (T1018): Finding the other machines on the network. | Discovery: looking around | The record describes internal network reconnaissance as a consequence; an attacker would likely probe internal service addresses to map the environment. |

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:

> *Wanderer is a self-hosted trail database for saving and sharing adventures. Prior to 0.20.0, when PUBLIC_PRIVATE_INSTANCE is not set to true, the unauthenticated POST /api/v1/trail/download handler passes the attacker-controlled JSON url field directly to event.fetch() and returns the fetched response. This allows requests to internal services such as db:8090 and search:7700, cloud metadata addresses, and other network destinations, exposing returned data and permitting internal network reconnaissance or denial of service. This issue is fixed in version 0.20.0.*

Versions of open-wanderer wanderer the record lists as affected:

- < 0.20.0

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-2026-71495
```

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-2026-71495
```

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 setting PUBLIC_PRIVATE_INSTANCE=true fully prevents unauthenticated access to the download endpoint in versions below 0.20.0, or only partially reduces exposure.
- Whether the cloud metadata addresses the SSRF can reach include credential-serving endpoints on the infrastructure a given deployment runs on.
- The advisory identifier GHSA-7vqq-mjjr-h9j5 is named in the v0.20.0 release notes; details beyond what the CVE record states are not reproduced in the sources provided.
- The GitHub source text says 'No CWEs' while the structured data lists CWE-918; the reason for this discrepancy is not stated in the sources.
- 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 read the vendor pages listed under Sources; nothing here has been tested.
- 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-2026-71495**: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/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 | None | Nothing can be altered. |
| Availability | High | Total loss of availability. |

## Appendix 2. Timeline

| Date | Event |
|---|---|
| 6 November 2026 | CVE record published by GitHub. |

## 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 |
|---|---|---|
| Instance below 0.20.0, PUBLIC_PRIVATE_INSTANCE not set to true, reachable from the internet | High | As soon as possible |
| Instance below 0.20.0, PUBLIC_PRIVATE_INSTANCE not set to true, internal network only | High | This week |
| Instance below 0.20.0, PUBLIC_PRIVATE_INSTANCE set to true | Medium | Next patch cycle |
| Instance at 0.20.0 or above | None | None for this CVE |

## Appendix 4. Definition of done

- Every open-wanderer wanderer 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-2026-71495: https://www.cve.org/CVERecord?id=CVE-2026-71495
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/open-wanderer/wanderer/security/advisories/GHSA: https://github.com/open-wanderer/wanderer/security/advisories/GHSA-7vqq-mjjr-h9j5
- Advisory or release notes read: github.com/open-wanderer/wanderer/releases/tag/v0.20.0: https://github.com/open-wanderer/wanderer/releases/tag/v0.20.0
- Reference in the CVE record: github.com: https://github.com/open-wanderer/wanderer/pull/1104
- Reference in the CVE record: github.com: https://github.com/open-wanderer/wanderer/commit/c371337b3db1d2895b5cad651046ef0ad4dfc802