

## SECURITY ADVISORY

# morpheus65535 bazarr: new CVE

CVE-2026-61826 · record published 30 October 2026

## Analysis Report

If you run Bazarr and anyone untrusted can reach it, update to 1.5.7-beta.14 or a later release now. The record gives no deadline. First find out whether and where it runs; if you do not run Bazarr ...

|             |                                |         |                                                         |
|-------------|--------------------------------|---------|---------------------------------------------------------|
| PREPARED BY | NamiQ                          | DATE    | 31 October 2026                                         |
| FACTS AS OF | 31 October 2026                | VERSION | 1.0                                                     |
| SEVERITY    | <b>Critical: CVSS 3.1 10.0</b> | 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/morpheus65535-bazarr-cve-2026-61826](https://namiq.io/insights/morpheus65535-bazarr-cve-2026-61826)

# The bottom line

*If you run Bazarr and anyone untrusted can reach it, update to 1.5.7-beta.14 or a later release now. The record gives no deadline. First find out whether and where it runs; if you do not run Bazarr, you can stop reading.*

# At a glance

| Fact            | Detail                                                                                                                                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product         | morpheus65535 bazarr (CVE-2026-61826)                                                                                                                                                                      |
| Severity        | Critical: 10 (CVSS 3.1)                                                                                                                                                                                    |
| Status          | A new CVE record, published by GitHub on 30 October 2026. Not on CISA's list of exploited vulnerabilities when we read it on 31 October 2026, which means nothing public says yet that anyone is using it. |
| Fixed in        | 1.5.7-beta.14 (the record says versions before it are affected; no other fixed version is named)                                                                                                           |
| Who looks first | Anyone running Bazarr, the subtitle companion to Sonarr and Radarr, on a version before the fix. Most exposed are installs reachable from the internet or from a network with untrusted users or devices.  |

# Does this apply to you?

Answer in order. Stop at the first no.

| Question                                                                                     | If no                                            | If yes                                  |
|----------------------------------------------------------------------------------------------|--------------------------------------------------|-----------------------------------------|
| Do you run Bazarr, on a server, a NAS or in a container?                                     | Nothing to do for this CVE.                      | Check the version (next question).      |
| Is your Bazarr version older than 1.5.7-beta.14?                                             | Nothing more to do for this CVE.                 | Check who can reach it (next question). |
| Can anyone untrusted reach the Bazarr web interface, from the internet or the wider network? | Lower priority: update at your next patch cycle. | Restrict access today and update.       |

## What it is

---

The record says Bazarr's Plex endpoints do not ask for an API key. Anyone who can reach the web interface can switch off its Plex link, store a key of their own choosing, or tie their own Plex account to your install, without logging in.

## Why it matters

---

Our reading is that this gives an outsider control of Bazarr's Plex connection without needing an account. The score is 10, and the sources show network access, low complexity, no privileges and no user action. The record also says an account the attacker controls can be bound to the instance, so your install could end up tied to a Plex account you do not own. The sources do not say how far that reaches beyond Bazarr itself.

## What the vendor's advisory says

---

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

- The GitHub advisory page lists CWE-306 and CWE-918 as well as CWE-352; the record lists CWE-352 and CWE-862.
- The advisory page gives the vector as network, low complexity, no privileges, no user interaction, changed scope, and high impact on confidentiality, integrity and availability.
- The advisory page credits ildkh as the finder and CyberKareem as the remediation verifier.
- The text we have does not name other flaws fixed in the same release, and gives no workaround.

## Things people will get wrong

---

- "It is not on the CISA list, so nobody is using it." The record is new and was not on CISA's list when read. That says CISA has not listed it, not that nobody is exploiting it.
- "It only matters if we use Plex." The description says anonymous callers can reach these endpoints without a PIN, account or state precondition. The sources do not say Plex must be set up first.
- "Bazarr needs an API key, so we are covered." The record says these Plex handlers omit the authentication check that normal APIs have, and no global hook makes up for it.

## 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 versions you run

---

- Find every Bazarr install, including containers, and note its version.
- Anything older than 1.5.7-beta.14 is in range, per the record.

```
docker ps --format '{{.Names}} {{.Image}}' | grep -i bazarr
systemctl list-units --type=service | grep -i bazarr
ps aux | grep -i [b]azarr
```

## Step 2: Reduce exposure until patched

---

- Take Bazarr off the internet and limit it to trusted machines. The flaw needs no login, so a password on the interface is not the fix.
- If you cannot patch today, ask your provider to restrict access in the meantime.

## Step 3: Update Bazarr

---

- Move to 1.5.7-beta.14 or later, the fixed version the record names.
- Note that this is a beta release tag; ask your provider which release they will install.

## Step 4: Check the result

---

- Confirm the running version is 1.5.7-beta.14 or later.
- Open the Plex settings in Bazarr and check the key, linked account and selected server are the ones you set.

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.

*Hello, we need to check our exposure to CVE-2026-61826 in Bazarr. Please tell us whether we run Bazarr, where, and which version. The record says versions before 1.5.7-beta.14 are affected and that the Plex endpoints can be used without logging in. If we are in range, please update to 1.5.7-beta.14 or later and restrict access until then. Please confirm the version and the fix to us in writing by the end of this week. Thank you.*

## The weakness behind it

---

The record classes this as CWE-352 and CWE-862.

## The sources, in their words

---

The CVE record:

*Bazarr is a companion application to Sonarr and Radarr. Prior to 1.5.7-beta.14, the `api\_ns\_plex` namespace in `bazarr/api/plex/oauth.py` omits `@authenticate` on its Resource handlers, while normal APIs require an API key and no global authentication hook compensates. Anonymous callers can invoke `POST /api/plex/oauth/logout` to clear credentials and disable the integration, or `POST /api/plex/apikey` to persist an attacker-selected key, without a PIN, account or state precondition. `POST /api/plex/oauth/pin` and `GET /api/plex/oauth/pin/<pin\_id>/check` additionally allow an attacker who completes a PIN with an attacker-controlled Plex account to bind that account's token to the instance. ...*

Versions of morpheus65535 bazarr the record lists as affected:

- < 1.5.7-beta.14

## What we do not know yet

---

- Whether anyone is exploiting this; the record is new and CISA had not listed it when read.
- Whether there is a workaround short of updating; the text we have names none.
- Whether Plex must be configured for an attacker to use the endpoints; the sources do not say.
- What else is fixed in 1.5.7-beta.14; no release notes are 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 31 October 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", "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-2026-61826:** 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                           |
|-----------------|---------------------------------|
| 30 October 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                               |
|-----------------------------------------------------------------------------------------|----------|-----------------------------------------|
| Version older than 1.5.7-beta.14, reachable from the internet                           | Medium   | Now; restrict access today, then update |
| Older version, reachable only from a home or office network with other users or devices | Medium   | This week                               |
| Older version, reachable only from one trusted machine                                  | Low      | Next patch cycle                        |
| Bazarr already at 1.5.7-beta.14 or later, or not run at all                             | None     | None for this CVE                       |

## Appendix 4. Definition of done

---

- Every morpheus65535 bazarr 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-2026-61826: <https://www.cve.org/CVERecord?id=CVE-2026-61826>
- CISA Known Exploited Vulnerabilities catalogue: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Advisory or release notes read: [github.com/morpheus65535/bazarr/security/advisories/GHSA-fvfcv-hh55-x3r4](https://github.com/morpheus65535/bazarr/security/advisories/GHSA-fvfcv-hh55-x3r4)
- Advisory or release notes read: [github.com/morpheus65535/bazarr/tree/v1.5.7-beta.14](https://github.com/morpheus65535/bazarr/tree/v1.5.7-beta.14)
- Reference in the CVE record: [github.com: https://github.com/morpheus65535/bazarr/commit/4bd29252feebd0803e84cc3ce1bdd24c3a076ed4](https://github.com/morpheus65535/bazarr/commit/4bd29252feebd0803e84cc3ce1bdd24c3a076ed4)
- Reference in the CVE record: [github.com: https://github.com/morpheus65535/bazarr/commit/f9a8a9514944be0e7b826e67cde042cebfe9c97e](https://github.com/morpheus65535/bazarr/commit/f9a8a9514944be0e7b826e67cde042cebfe9c97e)