contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

rucio: new CVE

CVE-2026-100397 · record published 17 November 2026

Analysis Report

If you run Rucio on a version below the fixed releases, upgrade to 35.9.1, 38.6.1, 40.4.2 or 41.1.1 this week, starting with any server that untrusted networks can reach. If you do not run Rucio …

PREPARED BY	NamiQ	DATE	17 November 2026
FACTS AS OF	17 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/rucio-cve-2026-100397

The bottom line

> *If you run Rucio on a version below the fixed releases, upgrade to 35.9.1, 38.6.1, 40.4.2 or 41.1.1 this week, starting with any server that untrusted networks can reach. If you do not run Rucio, stop reading.*

At a glance

Fact	Detail
Product	rucio (CVE-2026-100397)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by GitHub on 17 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 17 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	35.9.1, 38.6.1, 40.4.2, 41.1.1 (as the CVE record states them)
Who looks first	Teams that run a Rucio server (a scientific data management framework) on 1.14.0 or later but before a fixed release, above all where the API can be reached from outside the organisation.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Rucio server, or does a partner or provider run one for you?	Nothing to do for this CVE.	Find the version (next question).
Is the version 1.14.0 or later, and below the fixed release for your branch?	This CVE does not apply to that version, per the record.	Treat it as affected and check exposure.
Can anyone outside your trusted network reach the Rucio API?	Exposure is lower, but still upgrade; any insider or compromised host could use it.	Upgrade first and restrict access until then.

What it is

The record says a person with no account can request a short-lived SSH challenge token for any account name, then present it as an ordinary login token. The server accepts it, so they act as that account, including an administrative one.

Why it matters

The record gives a score of 10 and says no login and no user action are needed. Our reading is that this is account takeover, not data leakage alone: the attacker needs only an account name, can choose an administrative one, and could then read and change what that account controls. The weakness is CWE-287, Improper Authentication. The record does not say it is being exploited.

What the vendor's advisory says

We read one page on github.com. In short:

- The GitHub advisory page gives the CVSS 3.1 vector: network access, low complexity, no privileges, no user interaction, scope changed, high impact on confidentiality, integrity and availability.
- The page names thebatou as the finder and CWE-287 as the weakness.
- The text we have names no workaround and no other flaws fixed in the same releases.

Things people will get wrong

- "It is not on CISA's list, so we can wait." The record is new. The listing says nothing about whether anyone exploits it, and the record says no login is needed over the network.
- "Our users have strong passwords, so we are safe." The record says the attacker needs no credentials. They supply only an account name in a header.
- "Only the administrative account is at risk." The record says the attack works for an arbitrary account. An administrative account is named as one example.

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

- Ask whoever runs Rucio which servers exist and which version each one runs.
- Compare each version with the fixed releases: 35.9.1, 38.6.1, 40.4.2, 41.1.1.

```
pip show rucio
rucio --version
pip list | grep -i rucio
```

Step 2: Reduce exposure

- Limit who can reach the Rucio API to networks you trust until the upgrade is done.
- The sources we have name no workaround, so treat this as a stopgap, not a fix.

Step 3: Upgrade

- Move each affected server to the fixed release on its own branch, as the record states.
- Do not skip to a release the record does not name as fixed.

Step 4: Check the result

- Confirm the running version after the restart, not just the installed package.
- Ask your provider for the confirmation in writing.

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 have seen CVE-2026-100397 in Rucio. It lets an unauthenticated person obtain a login token for any account, including an administrative one. Please tell us whether we run Rucio anywhere, on which servers, and which version each runs. The fixed versions are 35.9.1, 38.6.1, 40.4.2 and 41.1.1. If any server is below its fixed version, please upgrade it and limit access to the API until then. Please confirm the versions and the fix in writing by the end of this week. Thank you.*

The weakness behind it

The record classes this as CWE-287.

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 record says an unauthenticated attacker reaches the API over a network, so this would likely be used to get in through an exposed Rucio service.
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	The attacker authenticates as a chosen existing account, so the activity would typically look like a legitimate user, including an administrative one.

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:

> *Rucio is a scientific data management framework. From 1.14.0 until 35.9.1, 38.6.1, 40.4.2, and 41.1.1, validate_auth_token in lib/rucio/core/authentication.py does not distinguish short-lived SSH challenge nonces from authentication tokens stored in the same token table. An unauthenticated attacker can request /auth/ssh_challenge_token for an arbitrary account by supplying X-Rucio-Account, then present the returned X-Rucio-SSH-Challenge-Token as X-Rucio-Auth-Token to authenticate to other API endpoints as that account, including an administrative account. This issue is fixed in versions 35.9.1, 38.6.1, 40.4.2, and 41.1.1.*

Versions of rucio the record lists as affected:

- >= 1.14.0, < 35.9.1
- >= 36.0.0, < 38.6.1

- >= 39.0.0, < 40.4.2
- >= 41.0.0, < 41.1.1

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-2026-100397
```

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-2026-100397
```

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 the flaw is being exploited. The record is new and CISA does not list it.
- Whether any workaround exists. The text we have names none.
- How an attack would show in Rucio logs. The sources do not say.

- 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 17 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-2026-100397: 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
17 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
A Rucio server on an affected version that is reachable from the internet	High	This week, before anything else
An affected server reachable only from an internal or partner network	Medium	This week
A server you cannot place on a fixed release yet	Medium	Restrict access now; patch as soon as possible
A Rucio server already on a fixed release	Low	Confirm the version, then no action
You do not run Rucio	None	None for this CVE

Appendix 4. Definition of done

- Every rucio 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-2026-100397: https://www.cve.org/CVERecord?id=CVE-2026-100397
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/rucio/rucio/security/advisories/GHSA-x585-4vv8-: https://github.com/rucio/rucio/security/advisories/GHSA-x585-4vv8-2mh2
- Reference in the CVE record: github.com: https://github.com/rucio/rucio/commit/4d4a58571ba853f3a55aef16ad9eb0944fce7483
- Reference in the CVE record: github.com: https://github.com/rucio/rucio/commit/4df924feb539ef789b3e78cbc00712ef8cdf606e
- Reference in the CVE record: github.com: https://github.com/rucio/rucio/commit/d7a3c2c2f933dce8edbcad07d8d076b9b782da35