contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

pulp_python: new CVE

CVE-2026-126984 · record published 26 November 2026

Analysis Report

Any team running pulp_python 3.6.0 through 3.38.1 with pull-through caching enabled should act this week; this CVE scores 10 and allows credential theft and repository poisoning with no …

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 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/pulp-python-cve-2026-126984

The bottom line

> *Any team running pulp_python 3.6.0 through 3.38.1 with pull-through caching enabled should act this week; this CVE scores 10 and allows credential theft and repository poisoning with no authentication required. The first step is to check whether the remote field is set on any Python distribution in your Pulp instance.*

At a glance

Fact	Detail
Product	pulp_python (CVE-2026-126984)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by Redhat on 26 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 26 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	3.11.10, 3.12.11, 3.13.9, 3.19.8, 3.27.10, 3.36.7, 3.38.2
Who looks first	Teams running Pulp with the pulp_python plugin where any Python distribution has the remote field set, enabling pull-through caching. The advisory says Red Hat Satellite ships only the generated Ruby API client and is not affected.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run the pulp_python plugin as part of a Pulp installation?	Nothing to do for this CVE.	Check whether pull-through caching is in use (next question).
Does any Python distribution in your Pulp instance have the remote field set?	Pull-through caching is not active; this CVE does not apply.	Check your version and apply the mitigation or patch (next questions).
Is the version you run in the affected ranges (3.6.0 through 3.38.1)?	Confirm you are on a fixed release; no further action needed.	Apply the fix: clear the remote field or update to a fixed release.
Is the content app reachable by untrusted network users or the internet?	Risk is reduced, but the fix still applies; complete it this patch cycle.	Treat this as urgent; the advisory says no login is needed to exploit it.

What it is

An attacker who can reach the content app can supply any URL as the download target. The server fetches it and returns the response. If the remote has a username and password, those credentials are sent to the attacker's chosen host.

Why it matters

The flaw is an SSRF: any network-reachable user can redirect the server's HTTP client to an arbitrary host. If the remote has credentials, the advisory says those are sent to that host. If the policy is immediate (the default) or on_demand, the downloaded file is stored and later served to all clients of the distribution. The advisory notes the content guard is unset by default, so no login is needed. Our reading is that the repository-poisoning path is the more serious concern for a package distribution operator: an attacker who controls what a distribution serves can affect every downstream consumer of that repository.

What the vendor's advisory says

We read one page on access.redhat.com. In short:

- The advisory says the vulnerable code was introduced in 3.6.0 when pull-through caching was added, and that saving downloaded files into the repository was added in 3.14.0.
- The advisory gives a mitigation that does not require a code update: clear the remote field on each Python distribution (set it to null). The advisory says pull-through caching stops and already-stored packages continue to be served.
- The advisory says Red Hat Satellite 6.16, 6.17, 6.18, and 6.19 ship rubygem-pulp_python_client, which is the generated Ruby API client, not the content app. Those streams are not affected.
- The advisory says a streamed remote policy also downloads the client-supplied URL and sends credentials when they are set, though it does not save the file into the repository.

Things people will get wrong

- If the remote has no username or password, the CVE does not apply. The advisory says credentials are only sent when the remote has them, but the SSRF and the repository-poisoning path both apply regardless of whether credentials are configured.
- Red Hat Satellite customers need to patch this. The advisory says Satellite ships only rubygem-pulp_python_client, the generated Ruby API client, not the content app. The vulnerable function is not present in those Satellite streams.

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 pulp_python version you run

- Check which release of pulp_python is installed on each Pulp server; the advisory says every release from 3.6.0 through 3.38.1 is affected.
- If you run multiple Pulp instances or separate content-app workers, check each one independently.

```
pip show pulp_python
```

Step 2: Check whether pull-through caching is in use

- List your Python distributions and check whether any have the remote field set to a non-null value; the advisory says that is the only configuration affected.
- If none have a remote set, this CVE does not apply to your installation.

Step 3: Apply the mitigation or update

- The advisory says clearing the remote field on each Python distribution stops the vulnerable download path; packages already in the repository continue to be served normally.
- If pull-through caching is required, the advisory says to update to a fixed release: 3.11.10, 3.12.11, 3.13.9, 3.19.8, 3.27.10, 3.36.7, or 3.38.2, according to the branch you run.

Step 4: Rotate credentials if the remote had a username and password

- The advisory says the remote's username and password are sent to any host the attacker supplies. If a credential was configured on the remote, treat it as potentially disclosed and rotate it at the upstream index.
- Review access logs at the upstream index for unexpected authorised requests that did not originate from your Pulp server.

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 are writing about CVE-2026-126984, a server-side request forgery flaw in the pulp_python plugin scored 10 out of 10. It affects all releases from 3.6.0 through 3.38.1. Please confirm whether we run pulp_python anywhere, and if so which version. We also need to know whether any Python distributions have the remote field set. Fixed releases are 3.11.10, 3.12.11, 3.13.9, 3.19.8, 3.27.10, 3.36.7, and 3.38.2. The vendor offers an interim mitigation without a code update: clear the remote field on each Python distribution. Please confirm in writing the installed version, whether pull-through caching is active, and whether the fix or mitigation is in place. We would like confirmation by 3 December 2026.*

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 record describes a network-reachable content-app endpoint exploitable without authentication via a crafted query parameter; this would typically map to exploitation of a public-facing application.
Data Manipulation: Stored Data Manipulation (T1565.001): Changing stored data without permission.	Impact: causing damage or disruption	From 3.14.0 the flaw lets a caller choose the file stored in the repository and served to later clients, which would likely constitute stored data manipulation of a package distribution.

Unsecured Credentials: Credentials In Files (T1552.001): Finding passwords or keys left in files.	Credential Access: stealing logins	Remote credentials stored in configuration are sent to an attacker-controlled host; this would likely be a path to obtaining credentials held in stored configuration.

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:

> *A **server-side request forgery** flaw has been found in the get_remote_artifact_url() function in pulp_python/app/models.py of the pull-through caching feature in the **pulp_python** package. The function uses the redirect query parameter from the client request as the URL to download. A network attacker or user who can reach the content app of a Python distribution that has a remote can choose that URL. The content app downloads it and returns the response. When the remote has a username and password, the download sends those credentials to the host in the URL. When the remote policy is immediate, the default, or on_demand, the file is saved into the distribution's repository and later ...*

Versions of pulp_python the record lists as affected:

- 3.6.0 up to, but not including, 3.11.10
- 3.12.0 up to, but not including, 3.12.11
- 3.13.0 up to, but not including, 3.13.9
- 3.14.0 up to, but not including, 3.19.8
- 3.20.0 up to, but not including, 3.27.10
- 3.28.0 up to, but not including, 3.36.7
- 3.37.0 up to, but not including, 3.38.2

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-2026-126984
```

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-2026-126984
```

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 say when each fixed release was published or whether it is currently available via the official package index.
- The sources do not say whether existing repository contents can be audited to identify files that were injected via this flaw rather than fetched legitimately.
- The sources do not describe what audit logging, if any, the content app writes for requests that use the redirect query parameter.
- 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 26 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-2026-126984: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N` 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	None	No effect on availability.

Appendix 2. Timeline

Date	Event
26 November 2026	CVE record published by Redhat.

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
pulp_python 3.6.0–3.38.1, remote field set on a distribution, content app internet-facing	Medium	Immediately; apply the mitigation today
pulp_python 3.6.0–3.38.1, remote field set, remote stores a username and password	Medium	Immediately; credentials are at risk of exfiltration
pulp_python 3.14.0–3.38.1, remote field set, policy is immediate or on_demand	Medium	This week; repository poisoning is possible from 3.14.0 onwards
pulp_python 3.6.0–3.13.9, remote field set, no credentials on the remote	Medium	This patch cycle; SSRF exists but file-saving was not yet present

Red Hat Satellite 6.16–6.19 running rubygem-pulp_python_client	None	No action needed for this CVE

Appendix 4. Definition of done

- Every pulp_python 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-2026-126984: https://www.cve.org/CVERecord?id=CVE-2026-126984
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: access.redhat.com/security/cve/cve-2026-126984: https://access.redhat.com/security/cve/cve-2026-126984
- Reference in the CVE record: access.redhat.com: https://access.redhat.com/security/cve/CVE-2026-126984
- Reference in the CVE record: bugzilla.redhat.com: https://bugzilla.redhat.com/show_bug.cgi?id=2584205
- Reference in the CVE record: github.com: https://github.com/pulp/pulp_python/pull/1429