contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Red Hat OpenShift Update Service: new CVE

CVE-2026-110697 · record published 11 November 2026

Analysis Report

If you do not run Red Hat Quay or an OpenShift integrated registry, nothing to do. Anyone who does and shares it across teams should update to the patched release now; the vendor's advisory scores ...

PREPARED BY	NamiQ	DATE	12 November 2026
FACTS AS OF	12 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	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/red-hat-openshift-update-service-cve-2026-110697

The bottom line

> *If you do not run Red Hat Quay or an OpenShift integrated registry, nothing to do. Anyone who does and shares it across teams should update to the patched release now; the vendor's advisory scores this 9.9 and needs only a basic account. Start by confirming which version is in use.*

At a glance

Fact	Detail
Product	Red Hat OpenShift Update Service (CVE-2026-110697)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by Redhat on 11 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 12 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	Red Hat Quay 3.9.28, 3.10.28, 3.12.24, 3.14.10, 3.15.9, 3.16.7, 3.17.7, or 3.18.3, per the vendor's advisory. Quay.io has already been fixed by Red Hat.
Who looks first	Teams and service providers running Red Hat Quay shared across more than one organisation or team. Single-tenant deployments face lower risk but are not exempt if untrusted users can create namespaces.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Red Hat Quay or use OpenShift with an integrated container registry?	Nothing to do for this CVE.	Check whether the deployment is shared between teams (next question).
Is your Quay instance shared between more than one team or organisation?	Risk is lower; still check your version and restrict namespace creation.	Check which version you are running (next question).
Can any authenticated user create a new namespace or organisation?	Risk is reduced; monitor for unexpected robot account activity.	Check whether your version is below the fixed release (next question).
Is your Quay version below the fixed release for your branch (e.g. below 3.9.28 / 3.10.28 / 3.12.24)?	No action needed for this CVE.	Update to the fixed version and rotate all robot account tokens.

What it is

An authenticated user creates a namespace name containing an underscore, which acts as a SQL wildcard matching other tenants' namespaces. The attacker can then list and retrieve decrypted robot account tokens from those other tenants and use them to read, push, or overwrite their container images.

Why it matters

The score of 9.9 reflects that only a low-privilege account is needed: no victim interaction, no elevated rights. The vendor's advisory says stolen robot tokens can be used to inject malicious images into CI/CD pipelines, putting the container supply chain across production clusters at risk. Our reading is that this matters beyond credential theft: an attacker who pushes a tampered image may gain code execution in every system that pulls from that registry, without directly accessing those systems.

What the vendor's advisory says

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

- The vendor's advisory gives fixed releases: 3.9.28, 3.10.28, 3.12.24, 3.14.10, 3.15.9, 3.16.7, 3.17.7, and 3.18.3. Quay.io is already patched.
- If immediate patching is not possible, the vendor recommends restricting namespace creation, rotating robot tokens for affected namespaces, and monitoring activity. It notes these steps reduce exposure but do not fix the flaw.

Things people will get wrong

- Only a namespace whose name exactly matches a victim's is a risk. An underscore in SQL LIKE acts as a single-character wildcard, so a name like 'a_corp' matches 'abcorp', 'axcorp', or any single character in that position—no exact match is required.
- Keeping Quay off the public internet makes us safe. The flaw requires only a valid account; an internal user or a compromised internal account is sufficient, regardless of whether Quay faces the internet.
- Quay.io customers need to apply this patch themselves. The vendor's advisory states Red Hat has already fixed Quay.io; only self-managed Quay deployments require a manual update.

How we would triage it

This is our judgement.

Step 1: Confirm whether Red Hat Quay is in use

- Check whether your environment includes a self-managed Red Hat Quay deployment or an OpenShift integrated registry; Quay.io is already patched and needs no action from you.
- If Quay is present, identify the installed version before deciding on urgency.

Step 2: Check whether the deployment is multi-tenant

- List the organisations in Quay; if more than one team or customer has an organisation on the same instance, treat it as multi-tenant and act with high priority.
- Review who has permission to create new organisations or namespaces; this determines whether the attack is reachable by non-administrative users.

Step 3: Update to the patched release

- The vendor's advisory names fixed versions: 3.9.28, 3.10.28, 3.12.24, 3.14.10, 3.15.9, 3.16.7, 3.17.7, or 3.18.3 depending on your branch. Apply the update for your branch.
- If you cannot update immediately, the vendor recommends restricting namespace creation, rotating robot tokens for any namespace whose name contains an underscore, and monitoring for unexpected image pulls or pushes.

Step 4: Rotate robot account tokens after patching

- After applying the patch, rotate all robot account tokens on the affected instance, paying particular attention to namespaces whose names could collide with an underscore-containing pattern.
- Confirm that no unexpected pulls or pushes occurred during the exposure window by reviewing registry audit logs.

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 have been made aware of a critical flaw in Red Hat Quay (CVE-2026-110697), scored 9.9, which allows an authenticated user to steal container registry credentials from other tenants and use them to modify images. Please confirm: (1) whether we run Red Hat Quay or an OpenShift integrated registry; (2) which version is deployed; (3) whether it is shared across multiple teams. If we are on an affected version (below 3.9.28, 3.10.28, 3.12.24, 3.14.10, 3.15.9, 3.16.7, 3.17.7, or 3.18.3 for the respective branch), please schedule an update and rotate all robot account tokens. We ask for written confirmation of the current version and planned update date by the end of this week.*

The weakness behind it

The record classes this as CWE-89.

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 a SQL injection in Quay's network-accessible API, exploitable by any authenticated user remotely; this would likely map to exploitation of the network-facing application.
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	Stolen robot account tokens would likely be used as valid credentials to authenticate to the registry, granting access without guessing passwords or compromising further accounts.
Data Manipulation: Stored Data Manipulation (T1565.001): Changing stored data without permission.	Impact: causing damage or disruption	The vendor's advisory says stolen tokens could be used to push or overwrite container images; this would typically constitute modifying stored data that downstream systems consume.

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 flaw was found in Quay where the robot account listing function constructs a SQL LIKE pattern from user-controlled namespace names without escaping wildcard metacharacters. An attacker who creates a namespace containing an underscore character can match and retrieve robot accounts and their decrypted authentication tokens from other tenants' namespaces, leading to cross-tenant credential theft and unauthorized image operations.*

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-2026-110697
```

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-2026-110697
```

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 Quay's audit logs record which namespaces were queried through the vulnerable robot listing function, making it possible to review whether the flaw was used before patching.
- Whether the Quay Operator on OpenShift applies minor version updates automatically or whether manual action is always required.
- Whether Quay branches older than 3.9 are also affected; the advisory names fixed releases starting from 3.9.28 but does not address earlier branches.
- 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 12 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-2026-110697: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/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	Low	An ordinary account is enough.
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
11 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
Multi-tenant Quay deployment, any authenticated user can create namespaces, registry is network-accessible	Medium	immediately
Multi-tenant Quay deployment, namespace creation is restricted to administrators	Medium	this week
Single-tenant Quay deployment where only trusted internal users hold accounts	Low	next patch cycle
Using Quay.io, the Red Hat managed service	None	none for this CVE

Not running Red Hat Quay or OpenShift with an integrated registry	None	none for this CVE

Appendix 4. Definition of done

- Every Red Hat OpenShift Update Service 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-2026-110697: https://www.cve.org/CVERecord?id=CVE-2026-110697
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: access.redhat.com/security/cve/cve-2026-110697: https://access.redhat.com/security/cve/cve-2026-110697
- Reference in the CVE record: access.redhat.com: https://access.redhat.com/security/cve/CVE-2026-110697
- Reference in the CVE record: access.redhat.com: https://access.redhat.com/solutions/7149592
- Reference in the CVE record: bugzilla.redhat.com: https://bugzilla.redhat.com/show_bug.cgi?id=2552237