servicenow

Scope Certified Application Installation And Configuration Guide

Snyk Security for Application Vulnerability Response (3.2.0)

VERSION CONTROL

#	Document Version	Date	Owner	Document Status	Comments
1	1.0.0	8th August, 2022	Crest Data Systems	Complete	• Brand new integration for Snyk SCA vulnerability with ServiceNow AVR
2	1.1.0	10th Oct, 2023	Crest Data Systems	Complete	• Bi-directional integration for triaging vulnerabilities and exception management from ServiceNow to Snyk • New ability to close AVITs when the project gets deleted from Snyk • Added CWE information from Snyk into ServiceNow • Additional filtering options: IsUpgradable, IsPatchable, Source, Patched, Fixable, IsPinnable and IsFixed • Added support of Utah and Vancouver ServiceNow versions
3	2.0.0	18th March, 2024	Crest Data System	Complete	• Added SAST Integration support • Added Support for the EU and AU regions • Added filtering support for TargetReference and Status • Updated source_scan_id mapping to latest_issue_counts.updated_at • Added mapping for Exploit Maturity and cvss Score • Added more granular triaging check in ServiceNow
4	2.1.0	03rd July, 2024	Crest Data	Complete	• Added filtering support for Target Name, Environment, Tags, and Lifecycle • Added mapping for SCA and SAST issue titles in source notes and description field of AVIT, respectively. • Added mapping of target name of Snyk project in the correlation ID field of scanned application table • Added feature for bulk ignored AVIT from the Remediation task • Updated Target Reference filter label to Branch • Updated user-agent

					• Fixed disappeared SAST issue should get closed in ServiceNow AVIT • Fixed approval business rule work for only Snyk AVIT
5	2.2.0	28th Nov 2024	Crest Data	Complete	• Improved filtering for issues imported using the REST API by applying filter rules after import. • Improved filtering to allow an "OR" condition when selecting multiple filters (the previous default only allowed "AND"). • Improved bidirectional ignore feature such that AVITs manually closed in ServiceNow will add a permanent ignore in Snyk, or AVITs manually reopened will delete existing ignores in Snyk. • Improved performance of large-scale issues import by giving customers the ability to set a system property to select the REST (more efficient) or V1 API for fetching SCA issues. • Added support for Custom Snyk Base URL • Bug fixes • Added support for Xanadu
6	3.0.0	16th Dec 2024	Crest Date	Complete	• Added filtering support for Project Type. • Added IaC issues support in existing SCA integrations • Mapped the Last opened as First found in AVIT • Changed mapping of disclosureTime to first_detection_date in third-party.
7	3.1.0	Jun 24, 2025	Crest Data	Complete	• Added AVIT close and reopen based on project status • Restrict closing issue on Snyk if project is inactive • Added v2 condition builder for project query • Updated user agent to v3.1.0 • Added event trigger to close AVIT on Snyk • Updated API version to 2024-10-15 • Added validation to restrict filtering for 1000 projects if V1 is in use.
8	3.2.0	8th Aug 2025	Crest Data	Complete	• Added support of bidirectional updates from Exception rules. • Added mapping of source_exploitability for REST SCA • Minor Bug fixes

Contents

1. Overview

Snyk is a Developer Security Platform that integrates directly into development tools and automation pipelines. Snyk makes it easy to find, prioritize, and fix security vulnerabilities in code, dependencies, containers, and infrastructure as code. Backed by industry-leading vulnerability intelligence and designed by developers for developers, Snyk fits into your development workflow to add security expertise to your toolkit.

Snyk ServiceNow Application

This application imports Snyk Projects and Snyk Issues data into ServiceNow as Application Release, Scanned Applications, Application Vulnerable Item, Vulnerability, Application Scan Summary, and Package in ServiceNow. It provides a user-friendly dashboard for data visualization and supports filtering issues to be ingested.

1.1. Application features

The main features of the integration include:

1. Deliver Snyk security insights on vulnerabilities in open-source dependencies seamlessly into a ServiceNow workflow
2. Provide visibility into your development team's application security risk on both platforms
3. Enable AppSec managers to create automated workflow processes to minimize risk and guide developer teams to focus on the highest priorities.
4. Synchronize vulnerability exceptions between ServiceNow and Snyk
5. Calculate vulnerability risk and determine prioritization using ServiceNow's vulnerability calculators combined with Snyk's industry-leading intelligence
6. Consolidate vulnerabilities and security outcomes, giving security teams visibility into end-to-end workflow management
7. Bidirectional functionality to ignore and unignore vulnerabilities using the ServiceNow exception or false positive workflows from ServiceNow to Snyk
8. Support the US, AU, and EU regions of Snyk

1.2. Compatibility Matrix

ServiceNow Version:

- Xanadu, Yokohama and Zurich

Snyk API Version:

- REST for projects and Organizations, SAST, SCA, IaC(US/AU/EU region)
- V1/reporting for SCA & IaC Issues(US region)

2. Snyk App for Vulnerability Response

This section describes the procedure for downloading and installing the Snyk Security for AppVR application from the store.

2.1. Pre-Requisites

1. The user should have an Enterprise license to the Snyk Platform.
2. Your ServiceNow Redirect URL ("https://YOUR-INSTANCE.service-now.com/oauth_redirect.do") must be set up on the Snyk side for the Snyk App to be authorized with ServiceNow.
   Note: ***Contact servicenow@snyk.io to register your instance for the Snyk app. Please mention that the redirect URL needs to be added under ServiceNow Snyk Security for Application Vulnerability Response. This step is mandatory for new integration installations.***

2.2. ServiceNow Plugins

The following ServiceNow plugins must be activated:

Vulnerability Response (com.snc.sn_vul) - min version(24.1.5)

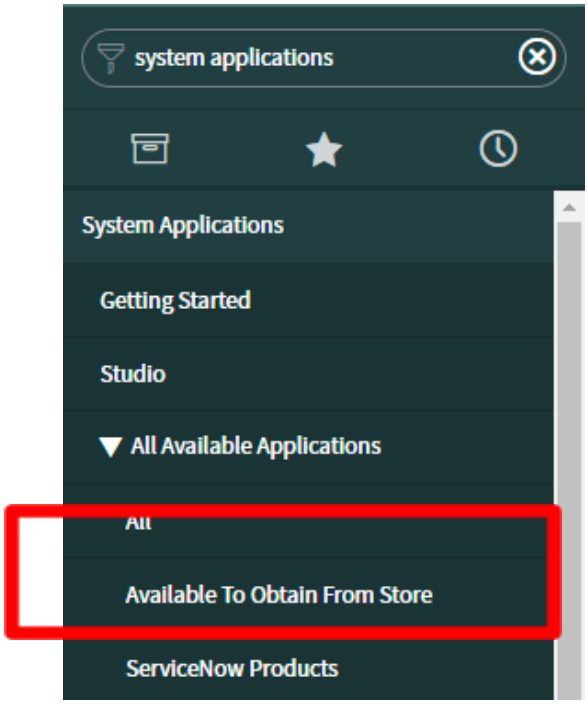
To install these plugins:

1. Log in to your instance with system admin credentials.
2. Navigate to "System Definition," and under it, select "Plugins" for your instance.
3. Search and install the above plugin.

2.3. Application Installation

Steps to install the application from the ServiceNow Store:

- Users with the System administrator(admin) role can install the application from the ServiceNow Store.
- Go to https://store.servicenow.com
- Search for the "Snyk Security for Application Vulnerability Response" on the search tab.
- Click on the Snyk Security for Application Vulnerability Response.
- Click on the "Get" button and enter the ServiceNow ID credentials.
- Once successfully added, open the instance and Navigate to Applications > All Available Applications > All.
- Find the application using the filter criteria and search bar.
- Next to the application listing, click Install.



3. Configuration Instructions for New Installation AND Upgrades

3.1. Update Required After App Install/Upgrade – Snyk Base URL Change

Background: Snyk has recently migrated its platform hosting for **new customers** to **AWS**. Existing customers will continue to be hosted on **Google Cloud Platform (GCP)**. New customer still has option to opt for GCP.

What's Changing in the ServiceNow App?
In this release of the ServiceNow Snyk Integration, the base URL will default to the new AWS URL: https://app.us.snyk.io

This means:

- If you are a new Snyk customer on AWS, you do not need to make any changes.
- If you are an existing or new Snyk customer on GCP, you need to update the base URL in your integration to continue syncing correctly.

If your Snyk organization is still hosted on GCP, follow these steps after upgrading the app:

- Open Global Settings and go to base URL and change URL to **app.snyk.io** for GCP

How to Know if You're on AWS or GCP?

If you're unsure which platform you're hosted on:

- Log in to your Snyk account and check the URL in your browser.
  - If it's `app.us.snyk.io`, you're on **AWS**.
  - If it's `app.snyk.io`, you're on **GCP**.

Important Note: Customers hosted in the `us.snyk.io` (AWS) region MUST use the REST APIs.

3.2. Permission and Roles

Note: By default **x_snyk2_snyk_vr_in.configure_integration** will be added under sn_vul.app_configure_integrations.

3.3. Create Users

Note: This step is optional. If you do not want to create a user, then System Admin can access the Snyk Application.
The ServiceNow platform admin creates the various users for the application.

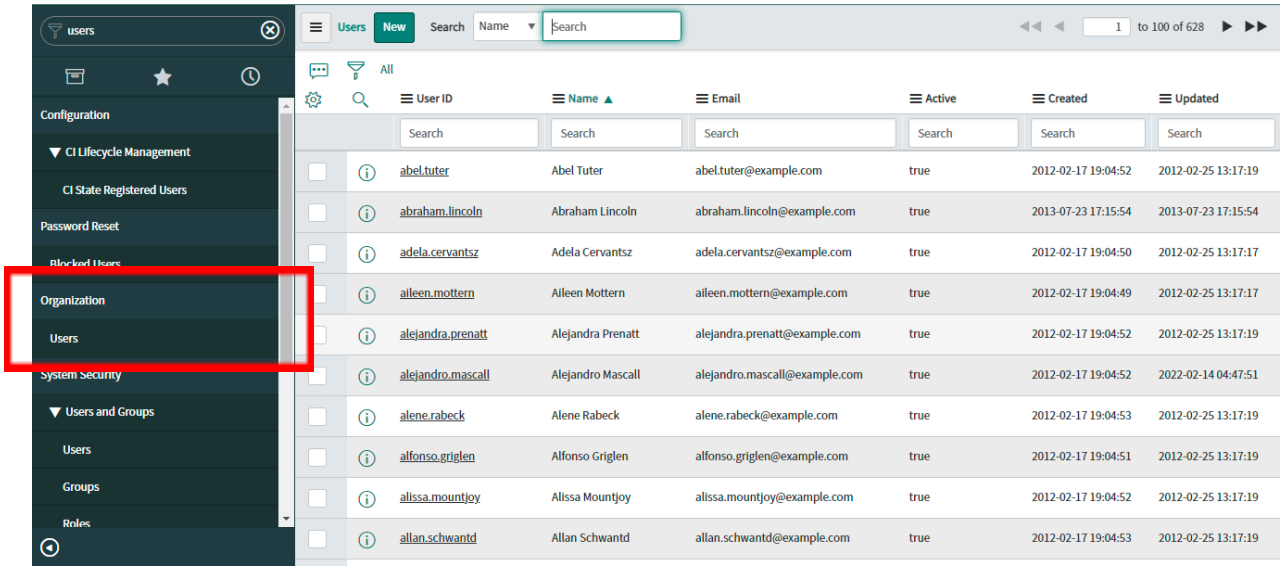
Username (for example)	Description	Role to be assigned
App Admin	This user will access the Snyk App for Application Vulnerability Response application, fetch the Data, and access various application modules.	• oauth_admin • sn_sec_cmn.admin • sn_vul.admin • sn_vul.app_exception_approver • sn_vul.app_false_positive_approver • sn_vul.app_manage_risk_score_configuration • sn_vul.app_read_assigned • sn_vul.app_configure_integrations • web_service_admin

Below is an example showing how to create an App Admin user and assign it to the "sn_vul.app_configure_integrations" role. Other users can be created similarly by giving them the appropriate roles.

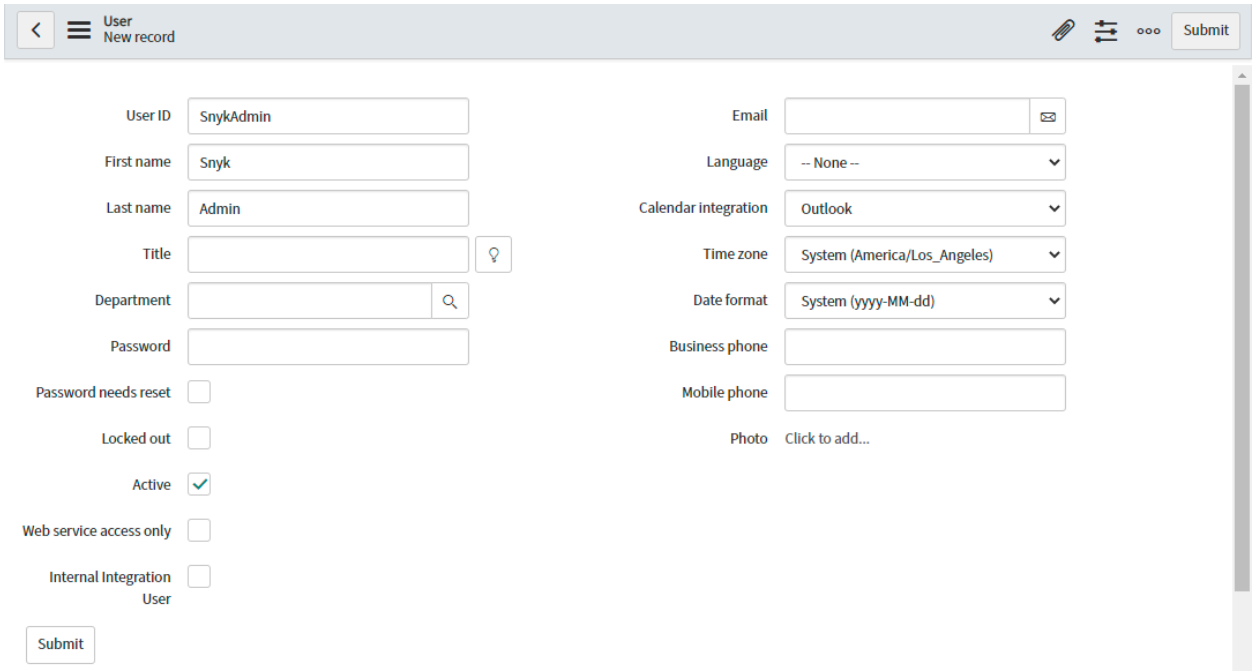
Role Required: System Administrator (admin)

Procedure:

- Navigate to "Organization" and select "Users" under it.
- Click the Users module.



- On the Users list that is displayed, click New. A new user form is displayed.



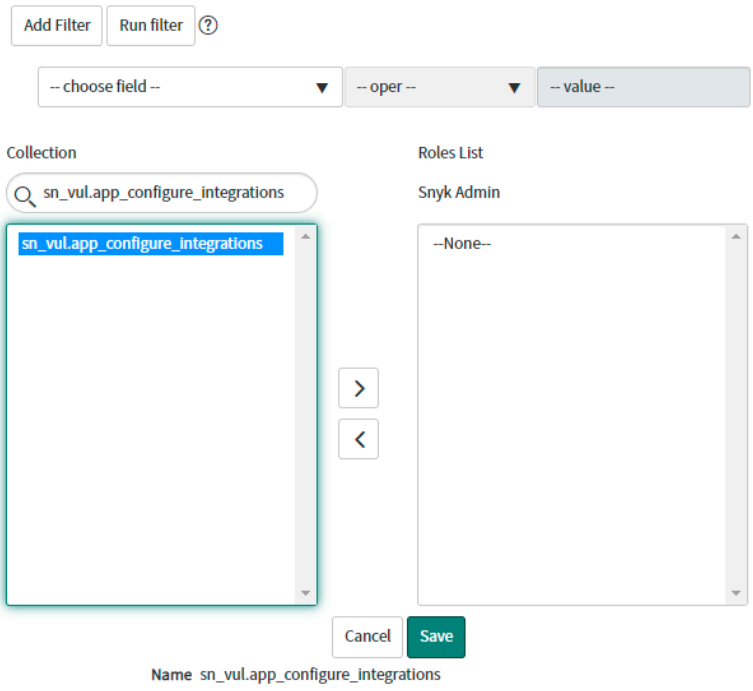
- Fill out the required details in the form.

Note: The values shown in the following table and figure are example values.

Field	Description
User ID	A unique user ID is required for the role in your ServiceNow Platform instance. An example is SnykAdmin

First Name	The person you are assigning
Last Name	The person you are assigning
Title	Job Title
Password	The unique password created for this user
Email	Unique email address

- Click Submit. Once submitted, you can assign the role.
- On the Users list, click on the name of the new user you created, such as Snyk Admin.
- In the user, the record goes to the Roles section, and click Edit.
- Select "sn_vul.app_configure_integrations" in the Collection column and move it to the Roles list. Similarly, users can add other roles to the user.



- Click Save.

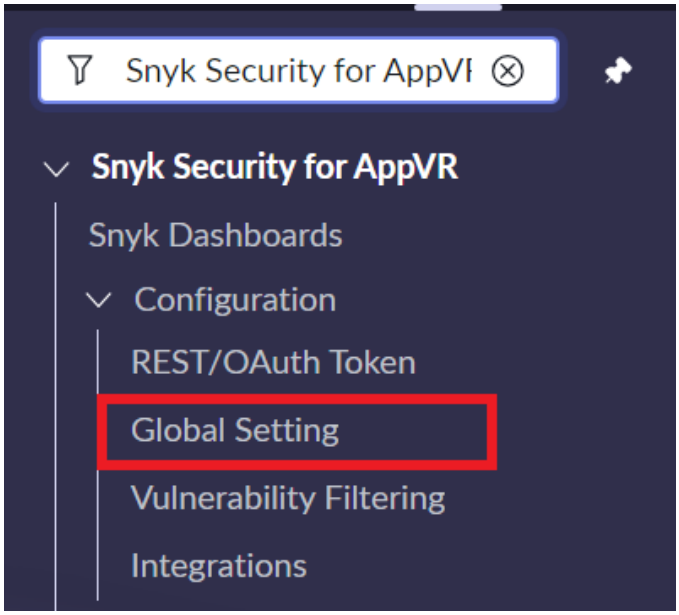
3.4. Global Setting

The global setting provides feasibility for defining project tag keys to populate Snyk projects into the CMDB table.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR" and select "Configuration."
3. Click on "Global Setting."



4. The Global setting page gets opened with the below default values

- "Base URL": https://api.us.snyk.io (Default)
    - Enter the Snyk BaseURL according to the region where your Snyk platform is deployed. Below are the valid BaseURLs
      US region Snyk BaseURL for GCP users : https://api.snyk.io
      US region Snyk BaseURL for AWS users : https://api.us.snyk.io
      EU region Snyk BaseURL : https://api.eu.snyk.io
      AU region Snyk BaseURL : https://api.au.snyk.io
      TenantURL: https://api.<tenant -name>.snyk.io

- "Project Tags": CMDBID
    - If a Snyk Project tag exists with the same key, such as "CMDBID," then the value of that tag is mapped with the source_app_id field in the CMDB table during the project import job.
    - If the tag is absent, then "project id"(unique ID) is mapped with the source_app_id field in the CMDB table.
- "Page size for projects": 100
- "Page size for SCA & IaC issues (US Region)": 1000

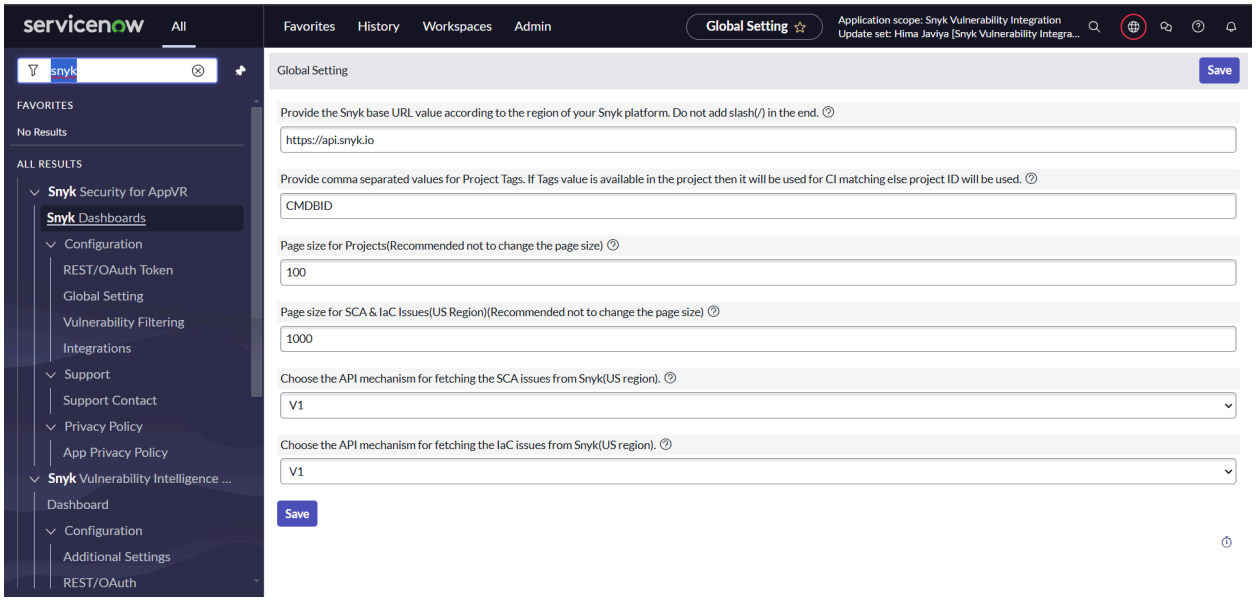
  Note: "Page size for SCA & IaC issue" property will not be used in SAST and SCA & IaC Vulnerability Import (Rest API - All region) Integration.

- "Choose the API mechanism to fetch the SCA issues from Snyk(US region).
    - **Important Note: Customers hosted in the `us.snyk.io` (AWS) region MUST use the REST APIs.**
    - There are two mechanisms for fetching SCA issues for the US region.

- V1 API
  - The V1 API has more options for filtering data to be imported, but it limits the number of projects that can be selected in the projects filter. You must use the REST API to apply a project filter for more than 1000 projects.
- REST API
  - Use this to fetch data for more than 1000 filtered projects.

- "Choose the API mechanism to fetch the IaC issues from Snyk(US region).
  - **Important Note: Customers hosted in the `us.snyk.io` (AWS) region MUST use the REST APIs.**
  - There are two mechanisms for fetching IaC issues for the US region.
    - V1 API
      - The V1 API has more options for filtering data to be imported, but it limits the number of projects that can be selected in the projects filter. You must use the REST API to apply a project filter for more than 1000 projects.
    - REST API
      - Use this to fetch data for more than 1000 filtered projects.

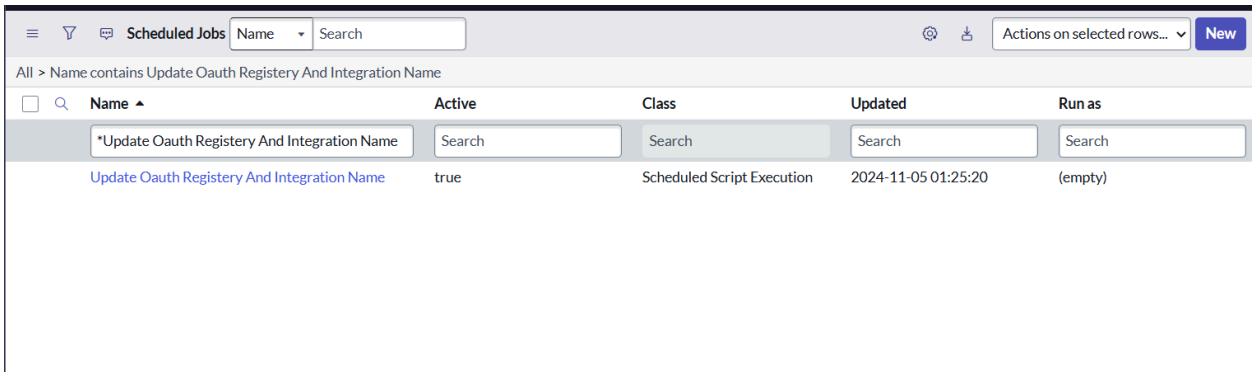
5. Provide the comma-separated project tag key to map the Snyk projects in the ServiceNow CMDB table. If a tag key is present on a project, that tag value will be used to map CI in discovered applications. For example, if "CMDBID: 1234" is present on a project, it will check scanned applications for any record with source_app_id as 1234. If found, it will map it to a newly created discovered application. Click the "save" button.



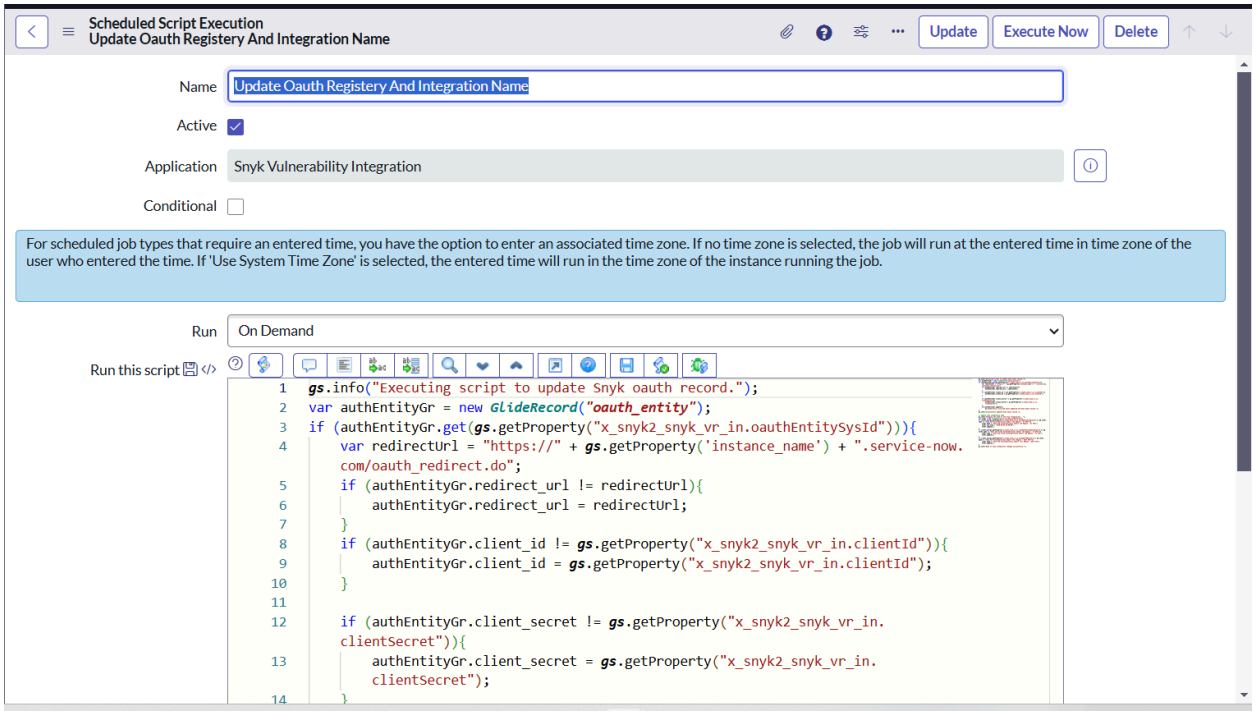
3.5. Run Scheduled Script (Mandatory Step for fresh Install, Upgrades, and Cloned instances)

Note: Please follow the steps below to update the mandatory application registry details for authentication.

1. Navigate to System Definitions -> Scheduled Job.
2. Search for Update Oauth Registry And Integration Name.



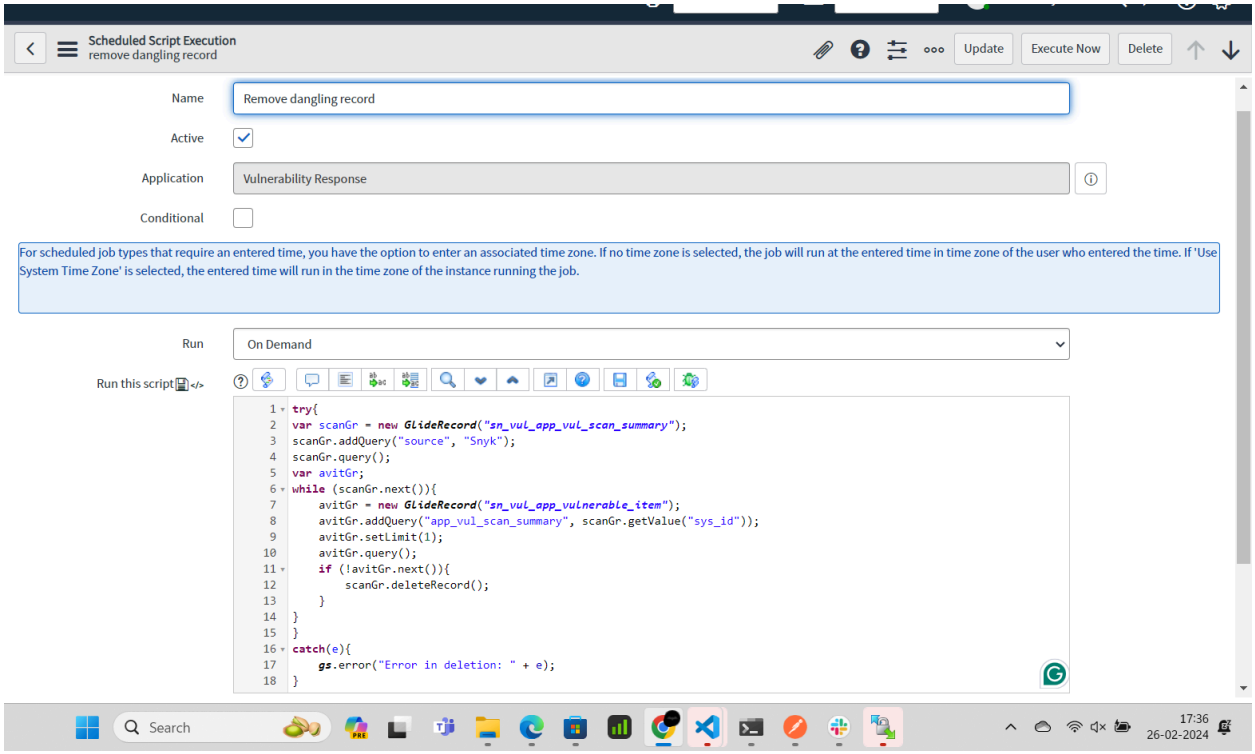
3. Click on that record.
4. Click on the Execute Now button.



Note: the steps below are optional to delete dangling scan summary records from the table. From 2.0.0, we use `latest_issue_counts.update_at` from projects as scan summary id instead of introducedDate in the issue.

If upgrading the Snyk application from 1.x to 2.x, follow the steps below to delete dangling records of scan summaries after fetching the data from Snyk after upgrading the integration.

1. Navigate to System Definitions -> Scheduled Job
2. Create a new scheduled job
3. Fill in the other details based on the screenshot below. ***(Ensure you create this script within the Vulnerability Response(VR) scope.)***



Here is the script

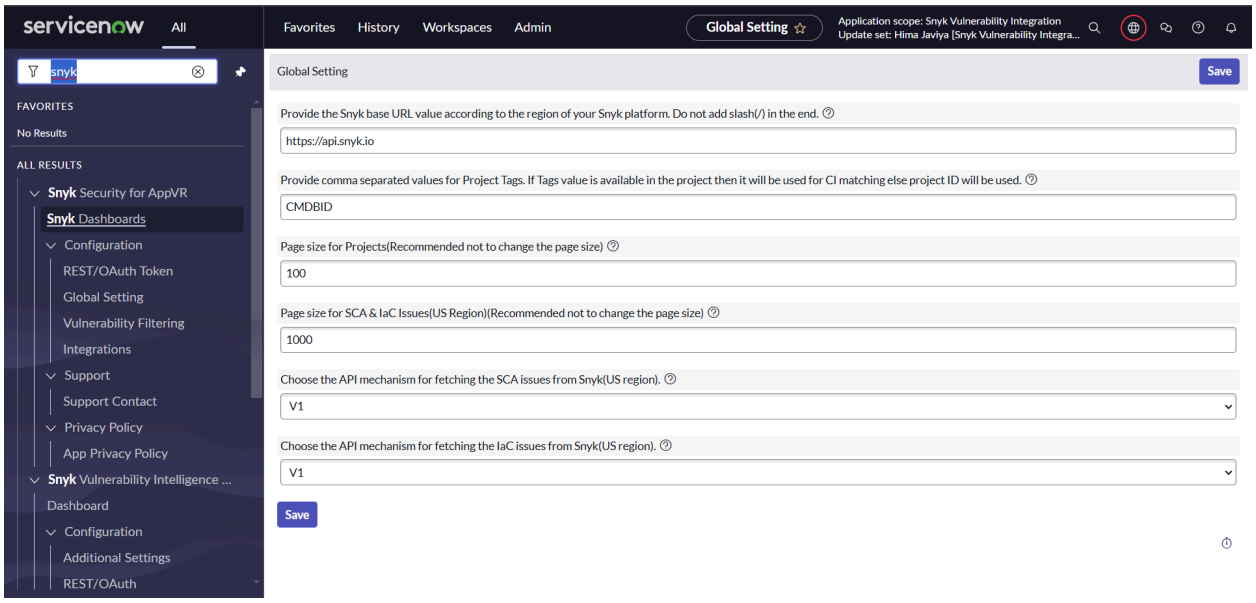
```
try{
var scanGr = new GlideRecord("sn_vul_app_vul_scan_summary");
scanGr.addQuery("source", "Snyk");
scanGr.query();
var avitGr;
while (scanGr.next()){
        avitGr = new GlideRecord("sn_vul_app_vulnerable_item");
        avitGr.addQuery("app_vul_scan_summary", scanGr.getValue("sys_id"));
        avitGr.setLimit(1);
        avitGr.query();
        if (!avitGr.next()){
                scanGr.deleteRecord();
        }
}
}
catch(e){
        gs.error("Error in deletion: " + e);
}
```

4. Click on the Execute Button to remove dangling scan summary records.

3.6. Generate REST/OAuth Token

Note: The steps below should be performed for AU and EU regions before generating a token.

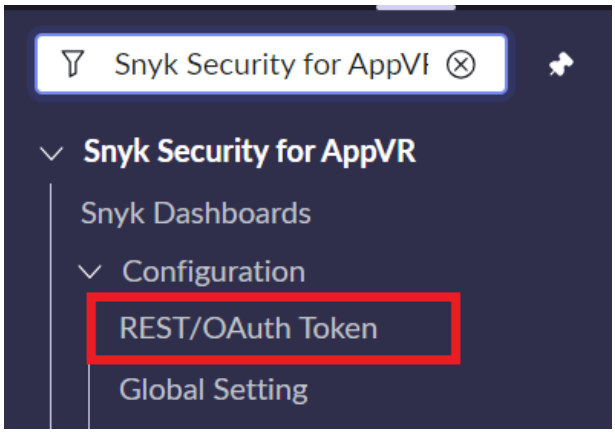
1. Login to the ServiceNow instance.
2. Navigate to Snyk Security For AppVR -> Global Settings.
3. Please enter the base URL value according to the region of your Snyk platform.
4. Click on Save.



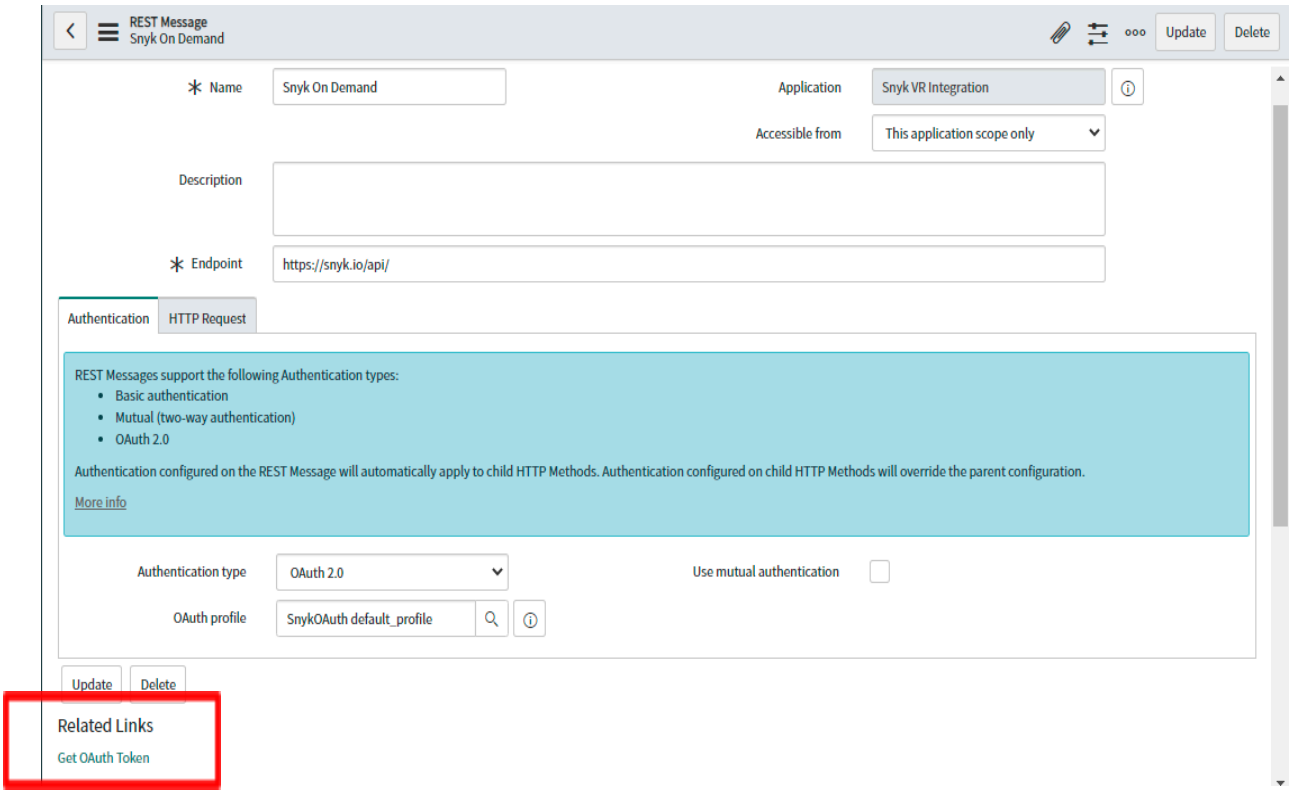
This section describes how to authorize Snyk Apps to fetch data from Snyk. This module will help the user generate the access token and regenerate a refresh token if either of the tokens expires.
Role Required: x_snyk2_snyk_vr_in.configure_integration, web_service_admin

Procedure:

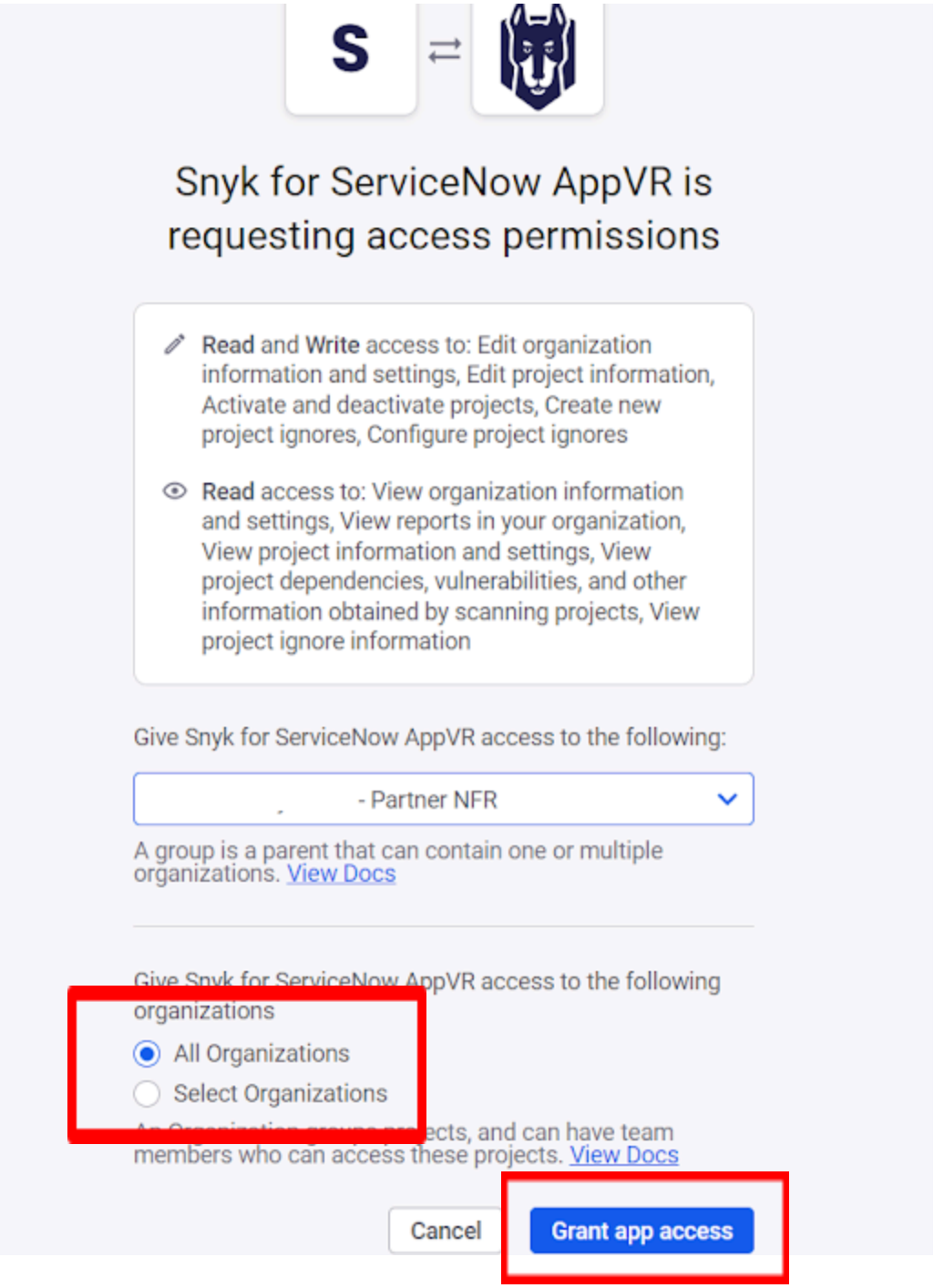
1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR."
3. Click on "Snyk Security for AppVR" under it, select "Configuration" and select "REST/OAuth Token" from the dropdown menu.



4. Click on the "Get OAuth Token" to generate the Access and Refresh tokens for the first time.
5. If the Refresh token expires, the user needs to follow all the steps from the beginning of this section to regenerate it.



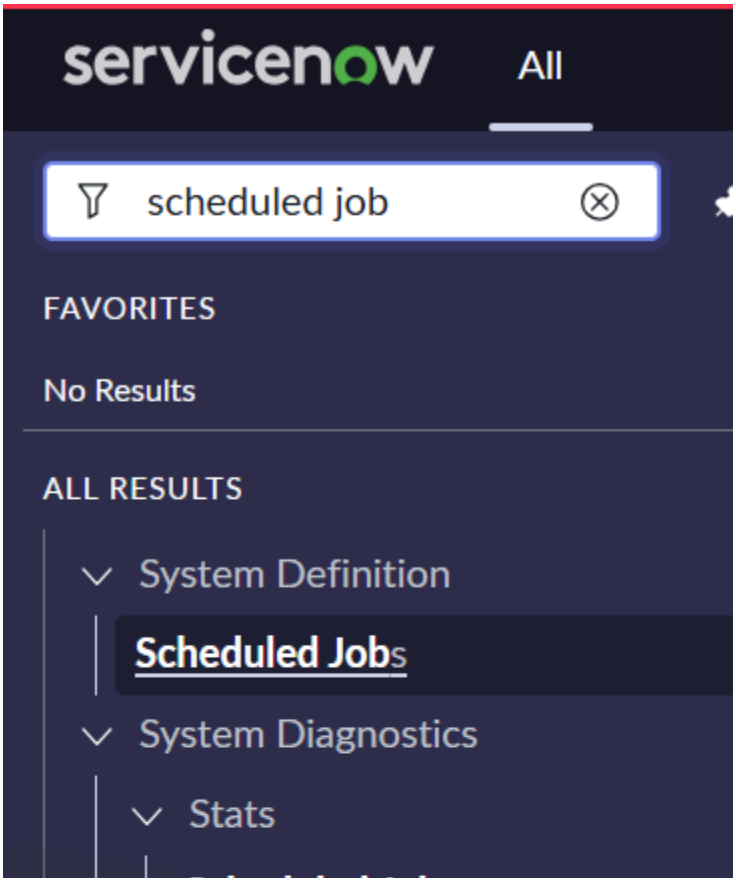
6. The system redirects the user to the Snyk App Authorization page after clicking "Get OAuth Token." Based on their requirements, users can provide access to all organizations or select a particular organization from the list.
7. To successfully authorize with Snyk Apps, the user must click "Grant app access."



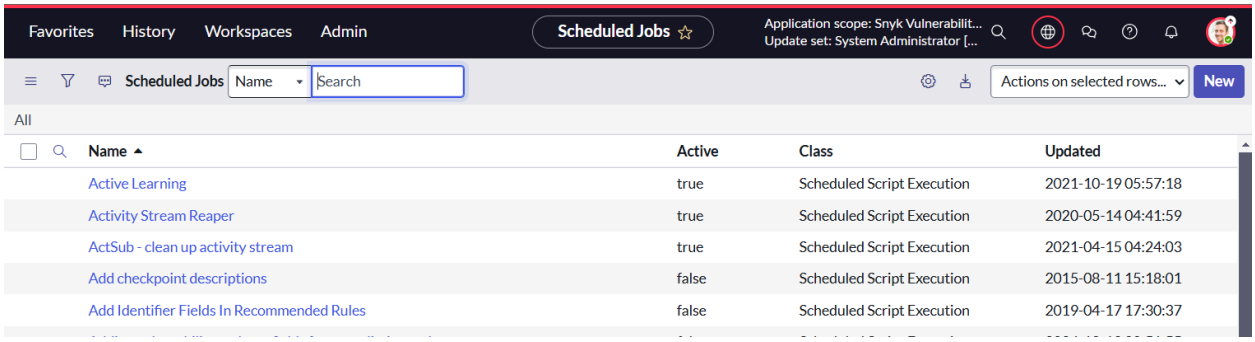
Note: This screenshot is for illustrative purposes only, your tenant is not accessible by any third party.

3.7. Add IaC Scan Type for IaC issues in AVIT Table (Only if you want to fetch IaC Issues)

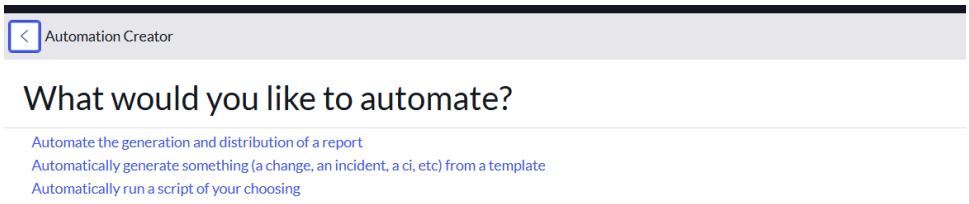
1. Navigate to Scheduled Jobs.



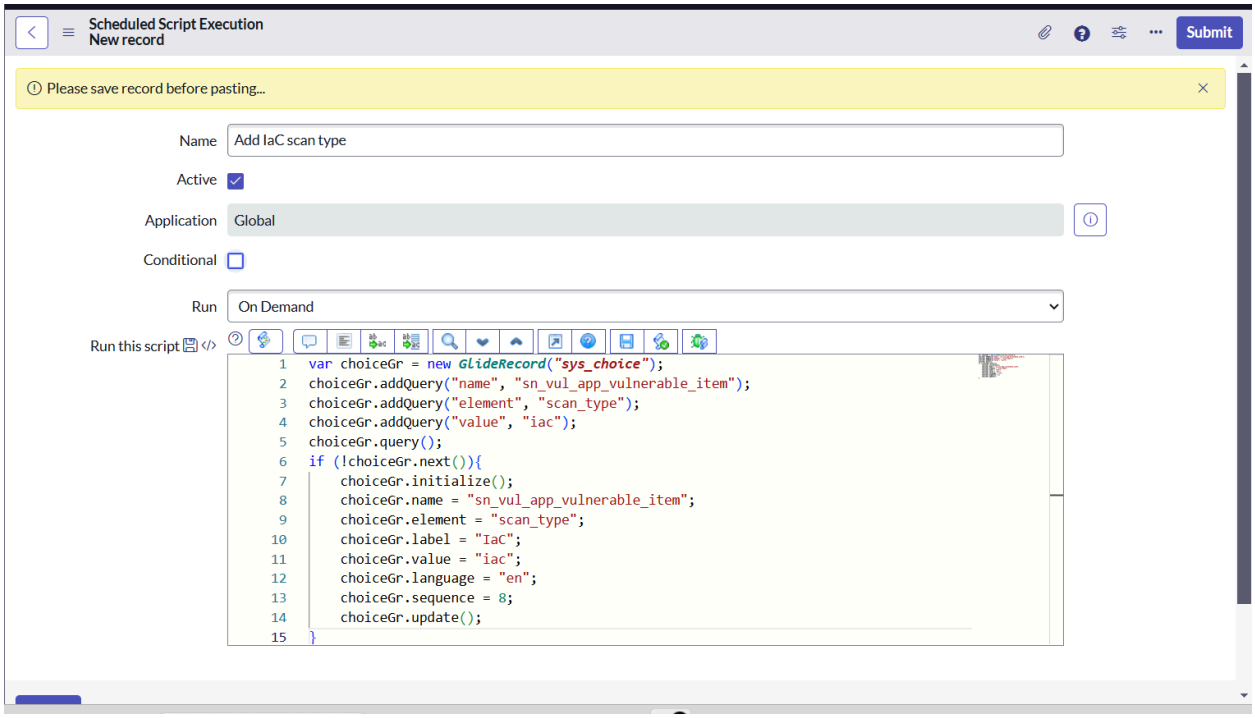
2. Click on the "New" button.



3. Click on Automatically run a script of your choosing.



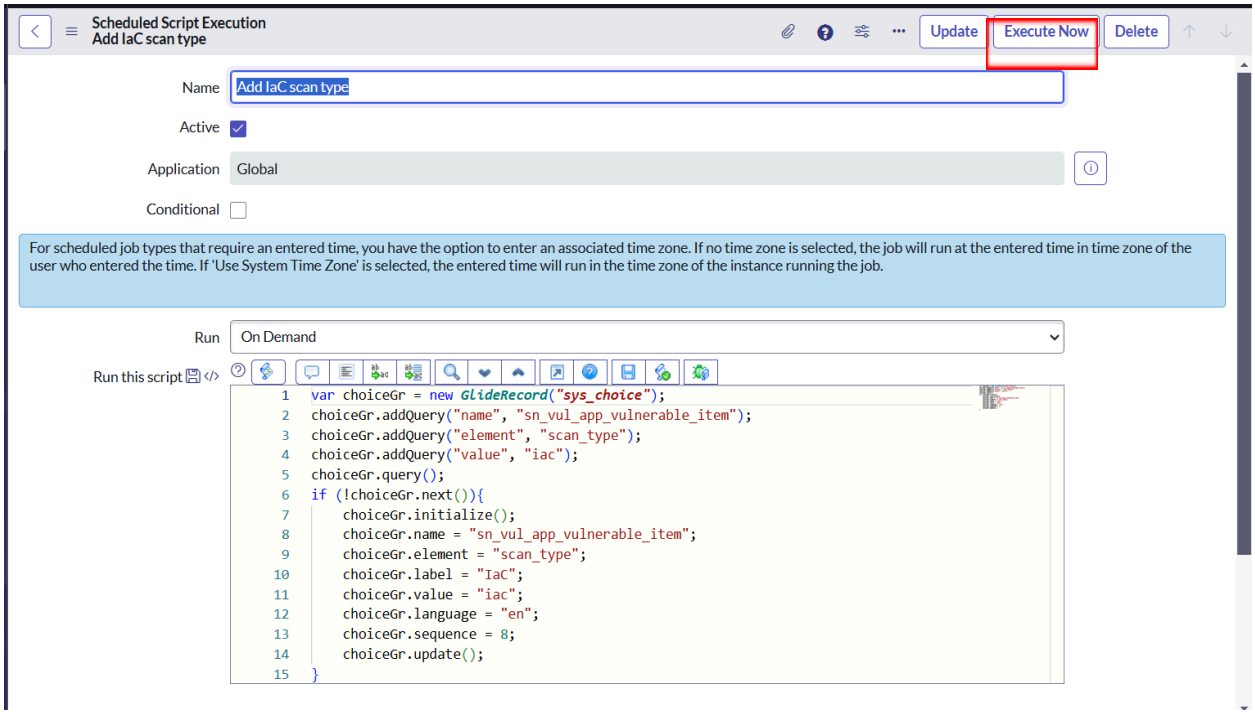
4. Add details of every field as mentioned in the below image.



5. Ensure the scope of your Application is **Global**.
6. Here is the script you can copy.

```
var choiceGr = new GlideRecord("sys_choice");
choiceGr.addQuery("name", "sn_vul_app_vulnerable_item");
choiceGr.addQuery("element", "scan_type");
choiceGr.addQuery("value", "iac");
choiceGr.query();
if (!choiceGr.next()){
    choiceGr.initialize();
    choiceGr.name = "sn_vul_app_vulnerable_item";
    choiceGr.element = "scan_type";
    choiceGr.label = "IaC";
    choiceGr.value = "iac";
    choiceGr.language = "en";
    choiceGr.sequence = 8;
    choiceGr.update();
}
```

7. Click on the Submit button.
8. Open the same scheduled job again and click on the Execute Now button.



4. Use Cases

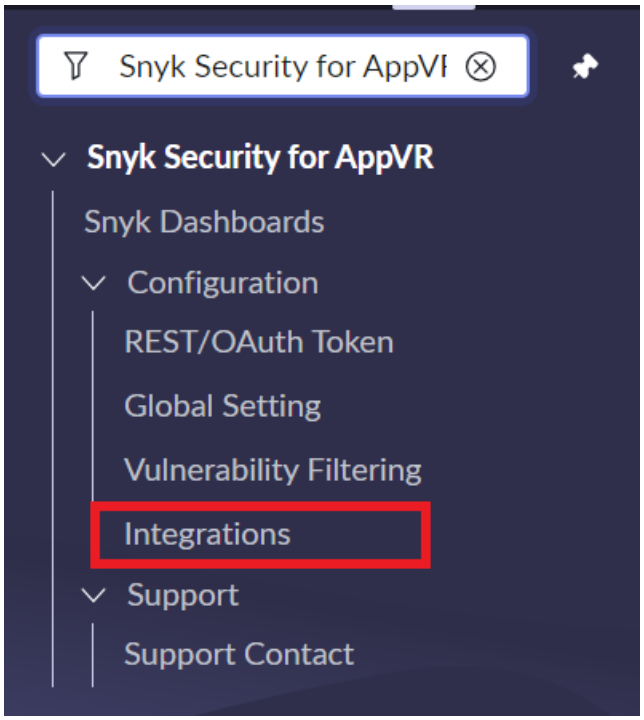
4.1. Fetch Projects from Snyk platform

"Snyk Security for AppVR" provides the functionality to fetch Projects from Snyk and populate them as an Application Release and Scanned Application in ServiceNow.

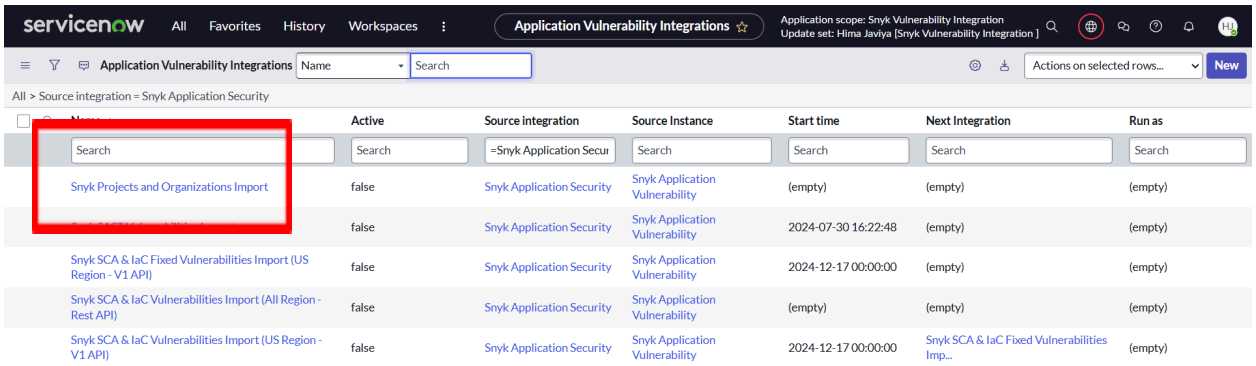
Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR," and under it, select "Configuration."
3. Click on "Integrations."

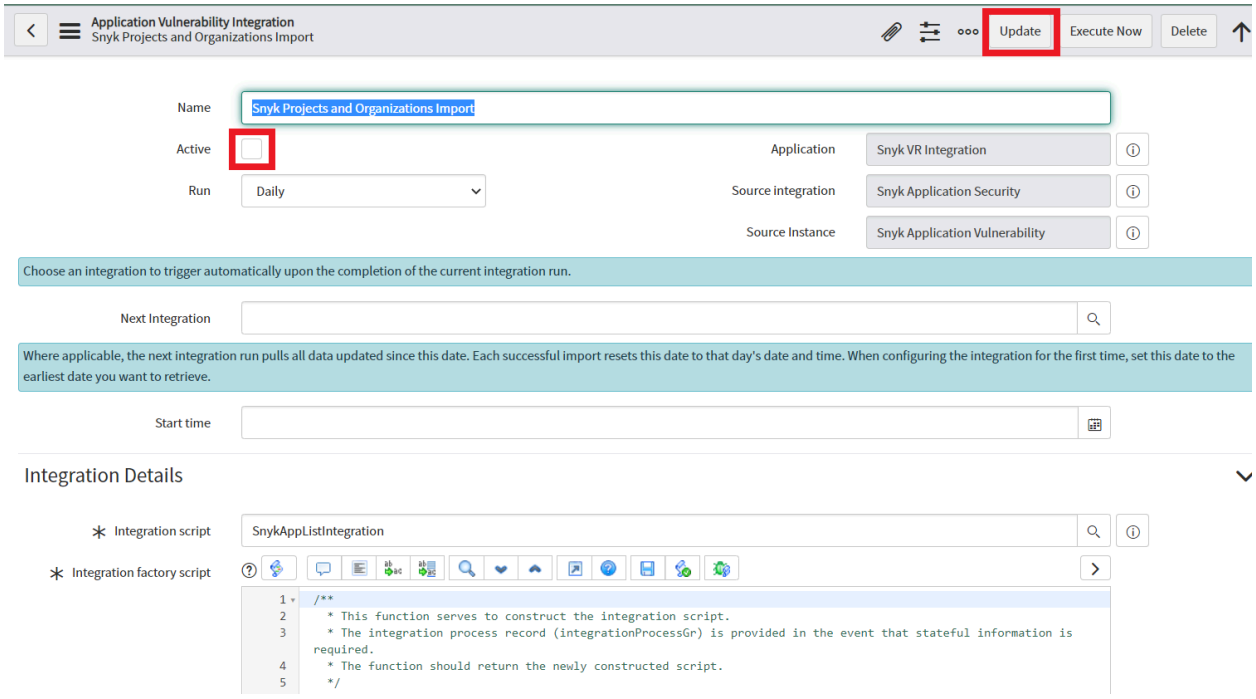


4. Select Integration with the name "Snyk Projects and Organizations Import" and the Source Instance value as the default provided by Integration Instance.

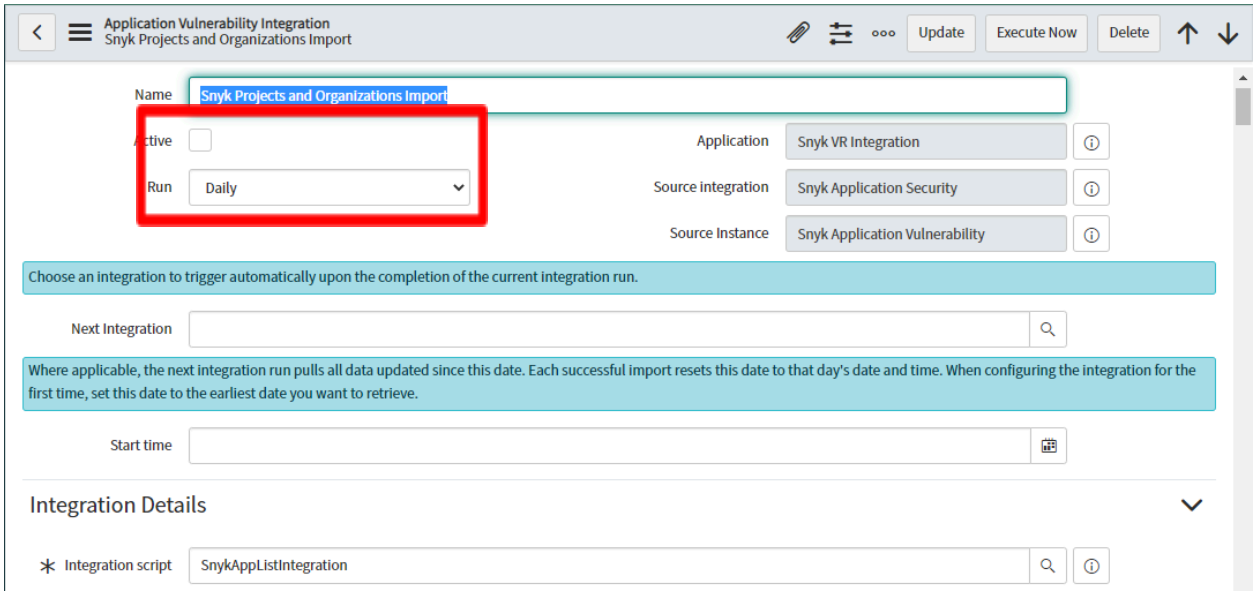


5. Activate the checkbox "Active." Click on the button "Update."

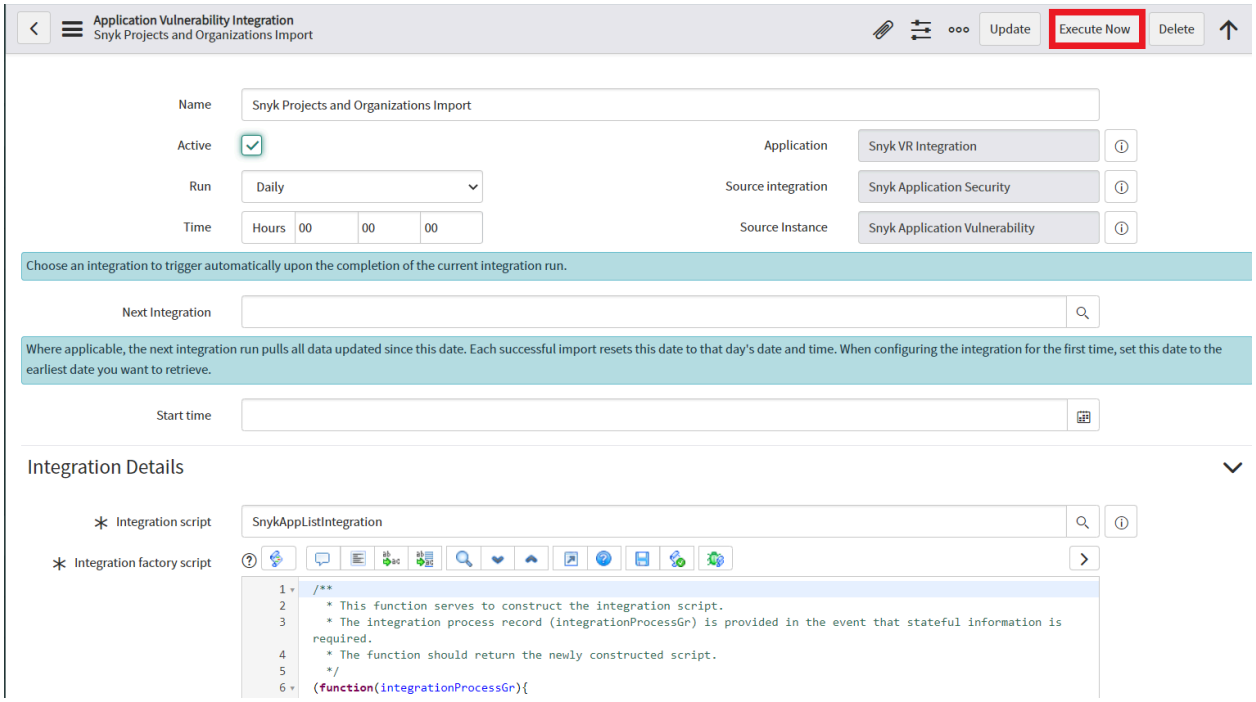
6. There is no need for a Start time**.** This integration will always fetch all projects and organizations.



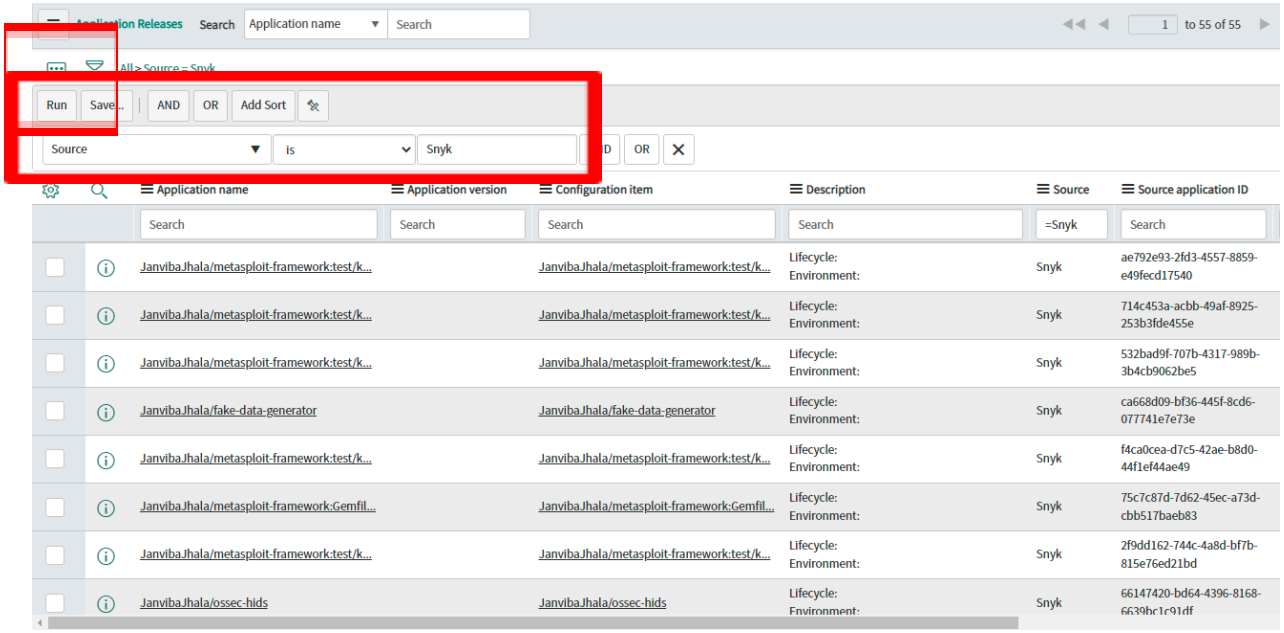
7. To fetch Projects according to a scheduled time interval, select the relevant option from the Run dropdown, set the Time, and click the "Update" button.



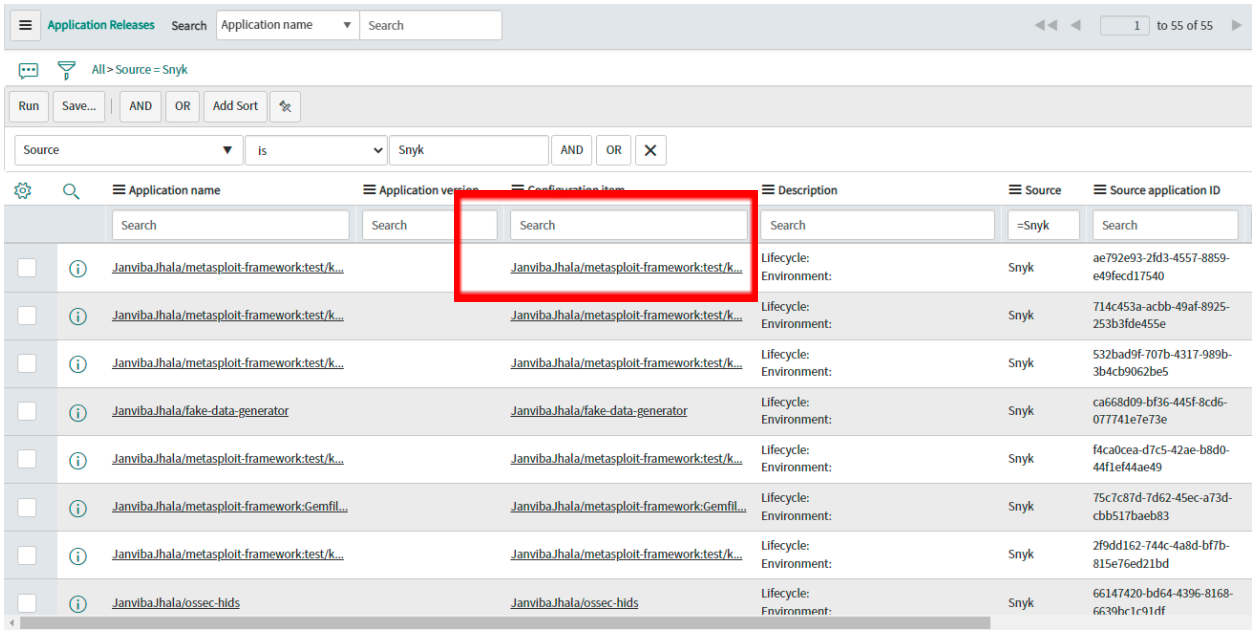
8. Open the Snyk Integration record. To fetch projects immediately, click on the "Execute Now" button.



9. Imported projects will be visible as Application Release (sn_vul_app_release).
10. Users will have to provide the filter, as "Source" is "Snyk," and then click on "Run" to view all the projects fetched from Snyk.



11. Click on Configuration Item to view the configuration item record.



4.2. Vulnerability Filtering

This section describes how to use filters to define which categories of issues to be imported from Snyk.

Note: The filters below do not work for Snyk Projects and Organizations Import integration.
Role Required: x_snyk2_snyk_vr_in.configure_integration

Filters:

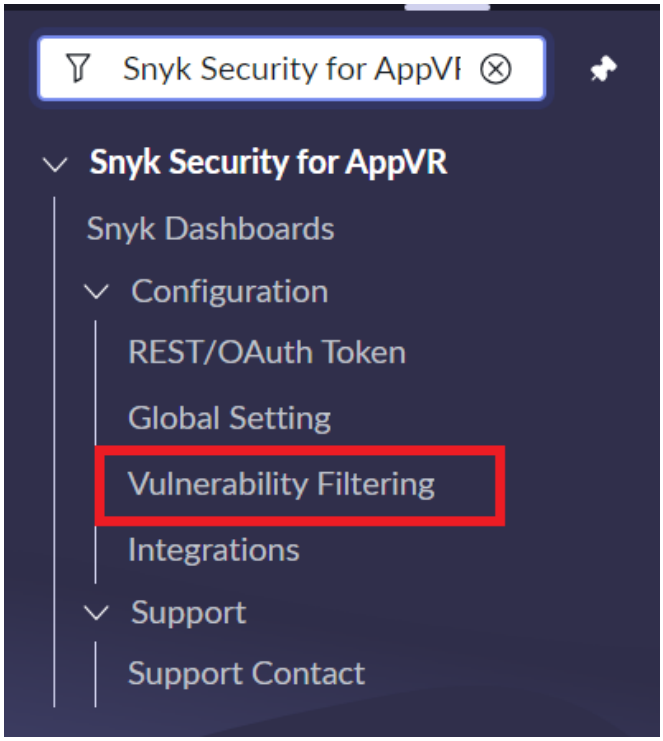
1) Organization
2) Projects
3) Projects Query
4) Project Type
5) Lowest Severity
6) Ignored
7) Minimum Priority Score
8) Maximum Priority Score
9) IsUpgradable
10) IsPatchable
11) IsFixed
12) Branch
13) Target Name
14) Environment
15) Lifecycle
16) Languages

17) Exploit Maturity
18) Source
19) Tags
20) Patched
21) Fixable
22) IsPinnable
23) Status
24) SCA IsFixable Condition

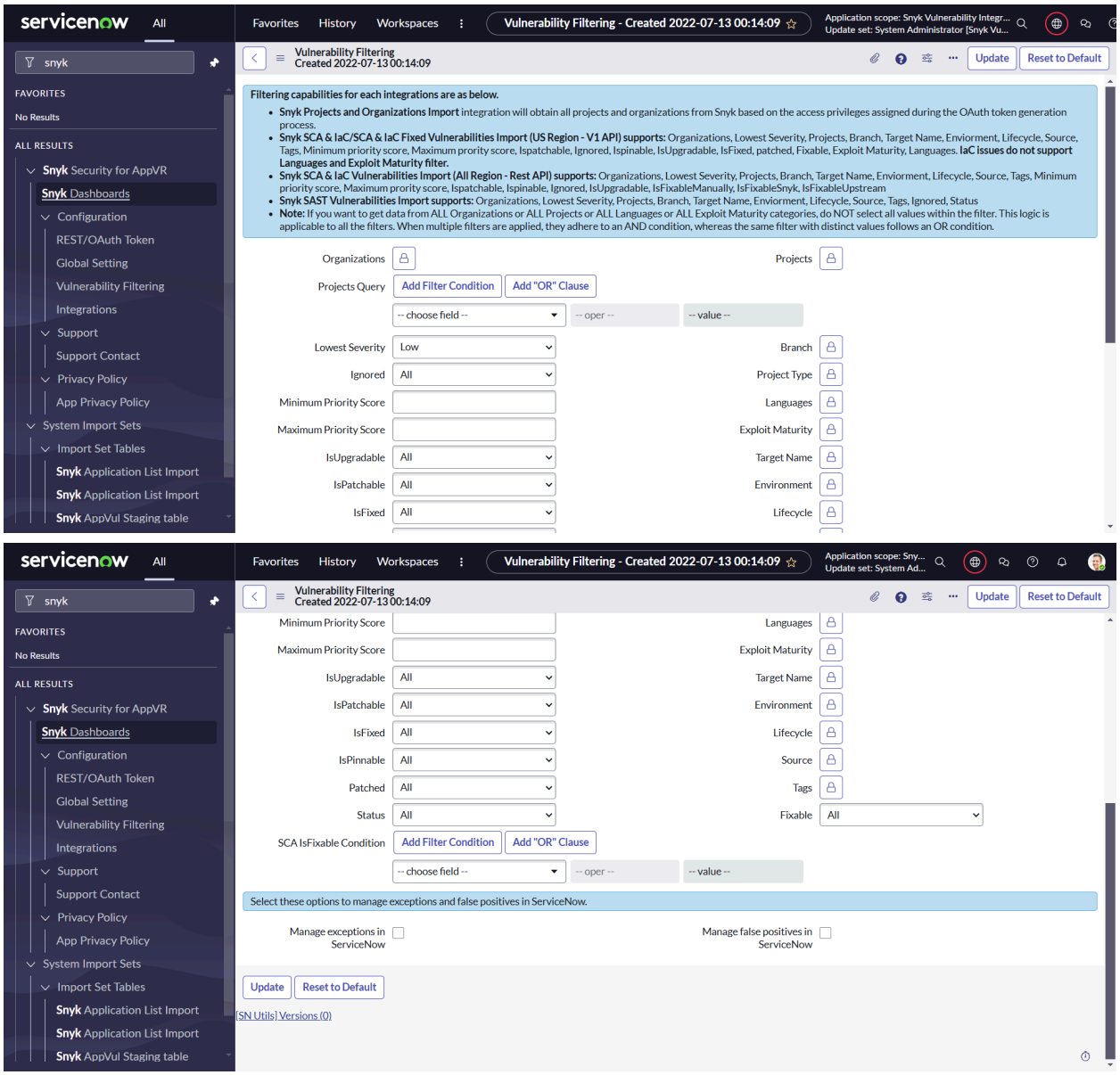
Note: If you're transitioning Snyk from version 1.1.0 to 3.x, it's necessary to execute the Snyk Projects and Organizations Import to access the benefits of the **Branch, Target Name, Environment, Lifecycle, and Tags** filter.

Procedure:

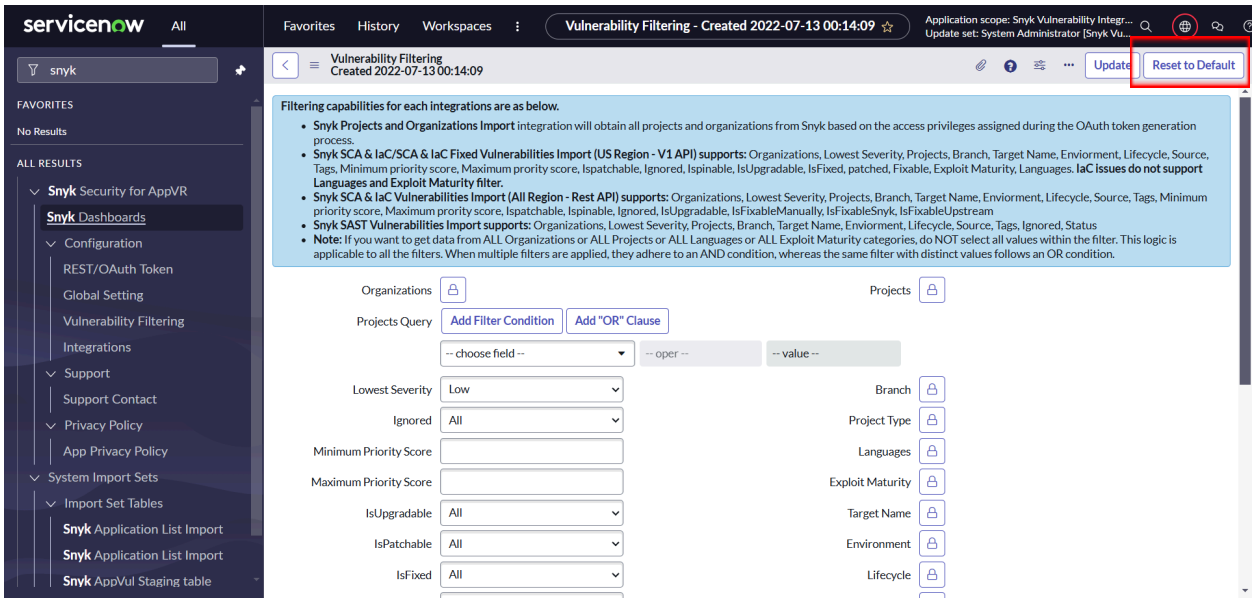
1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR" and select "Configuration."
3. Click on "Vulnerability Filtering."



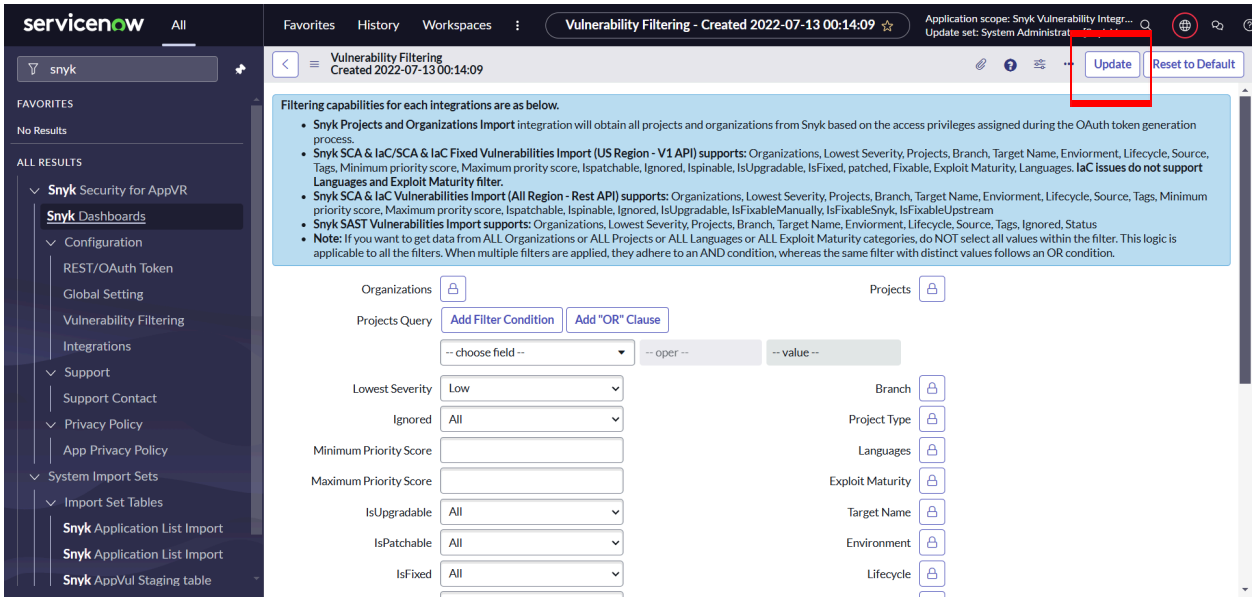
4. The Vulnerability Filtering form view gets opened with a default value for Lowest Severity as "Low," and a default value for Ignored, IsUpgradable, IsPatchable, Patched, Fixable, IsPinnable, IsFixed as "All," and the "Status" field is used for the SAST type issues/Vulnerability.
5. For the SAST integration, Ignored, Severity, and Status fields are used to filter the issues/Vulnerability.



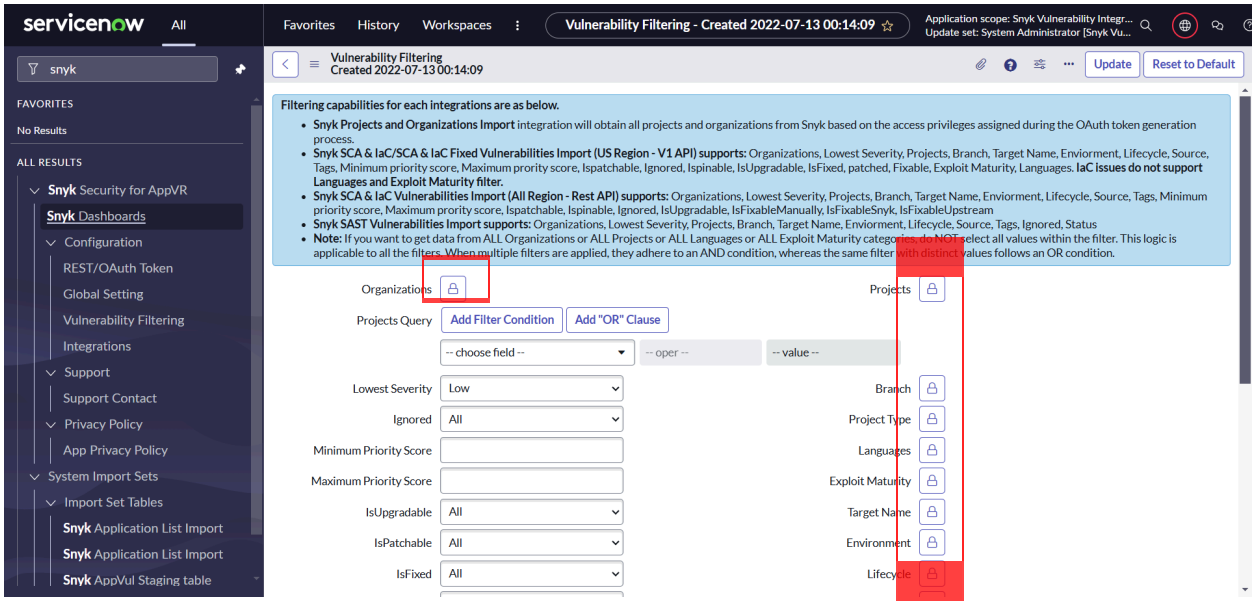
6. Users can reset the filters by clicking on the **Reset to Default** button.



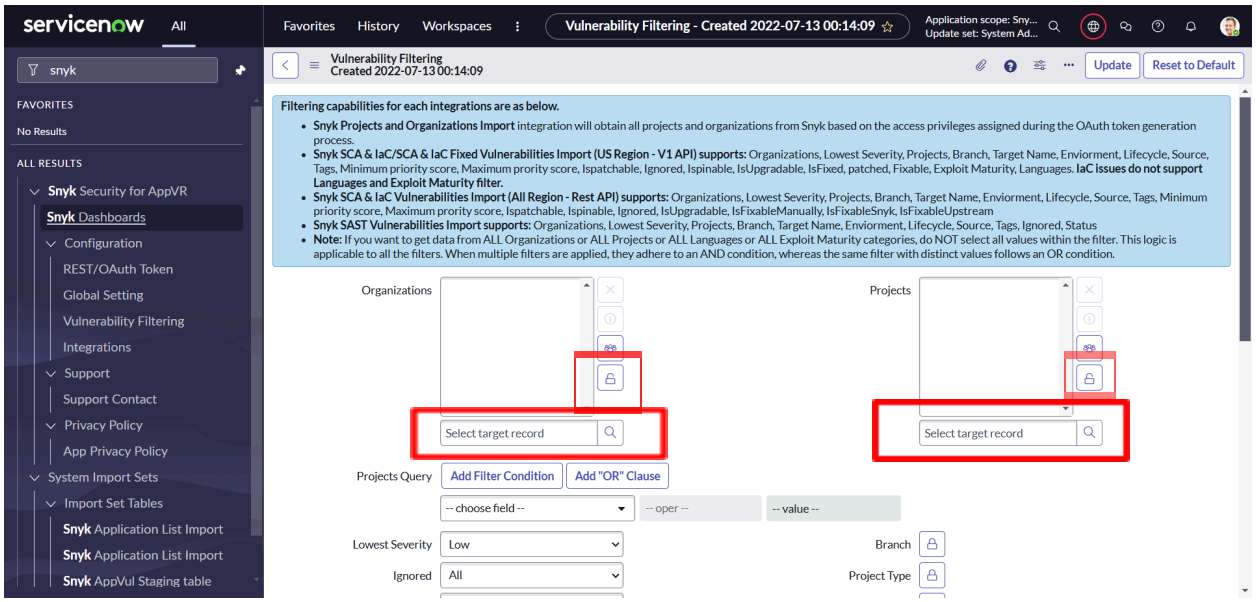
7. Users can update the existing record. Change the existing details and click on the update button.



8. Organizations, Projects, Languages, Branch, Target Name, Environment, Lifecycle, Exploit Maturity, Tags, and Source Filters can be modified by clicking the Lock button.

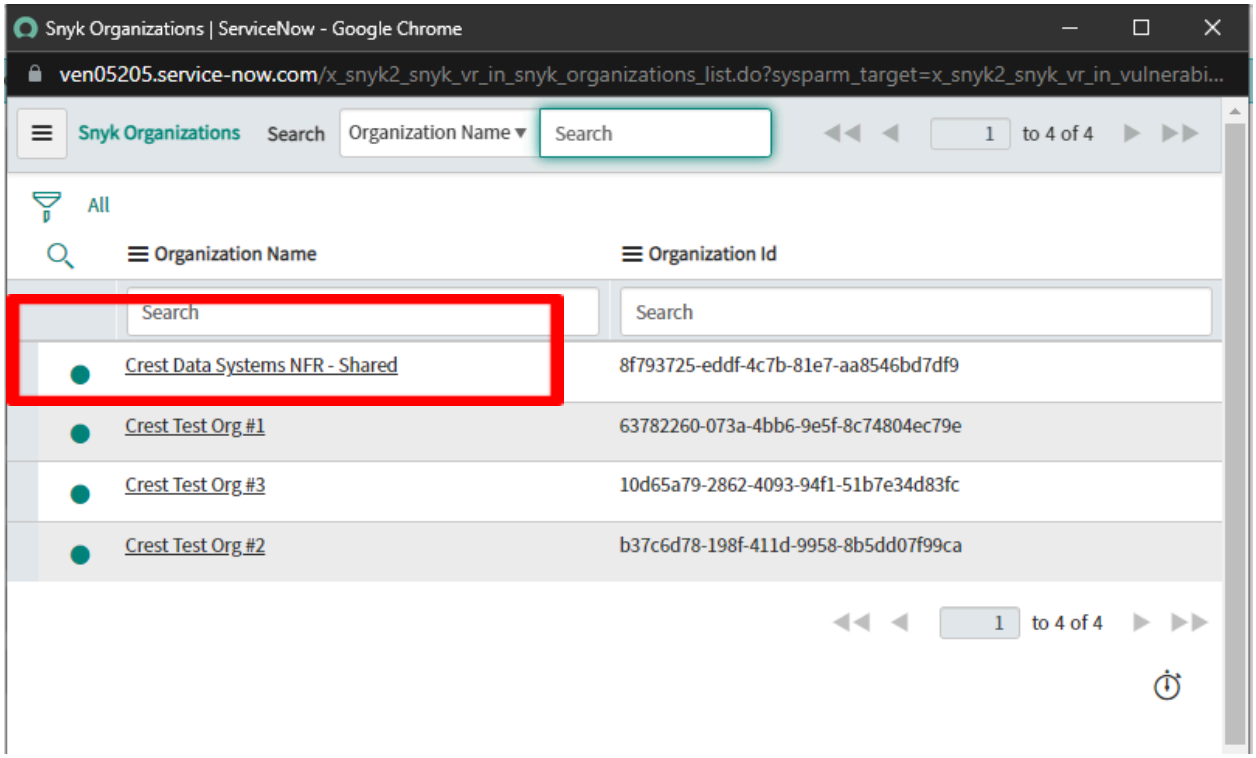


9. If users want to select a single organization or project from the list, they must click on the icon below.

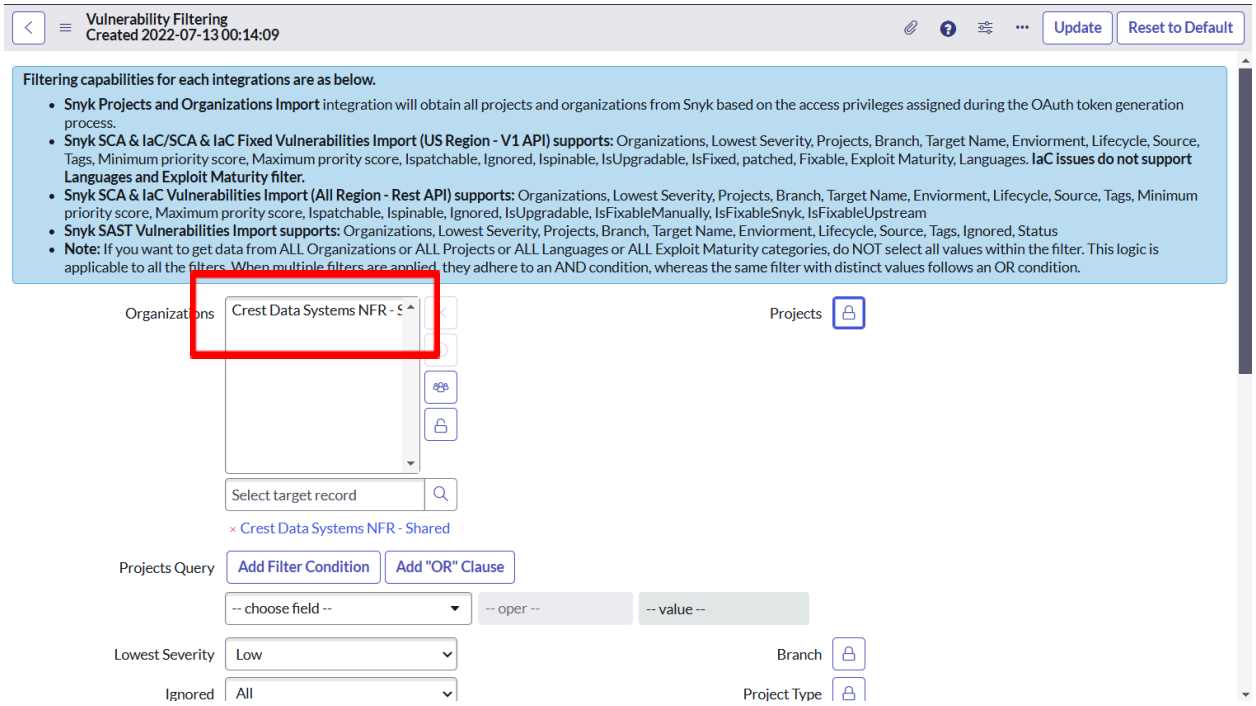


10. Clicking on the above icon will open up the list of organizations and projects from which users can select organizations and projects one at a time.

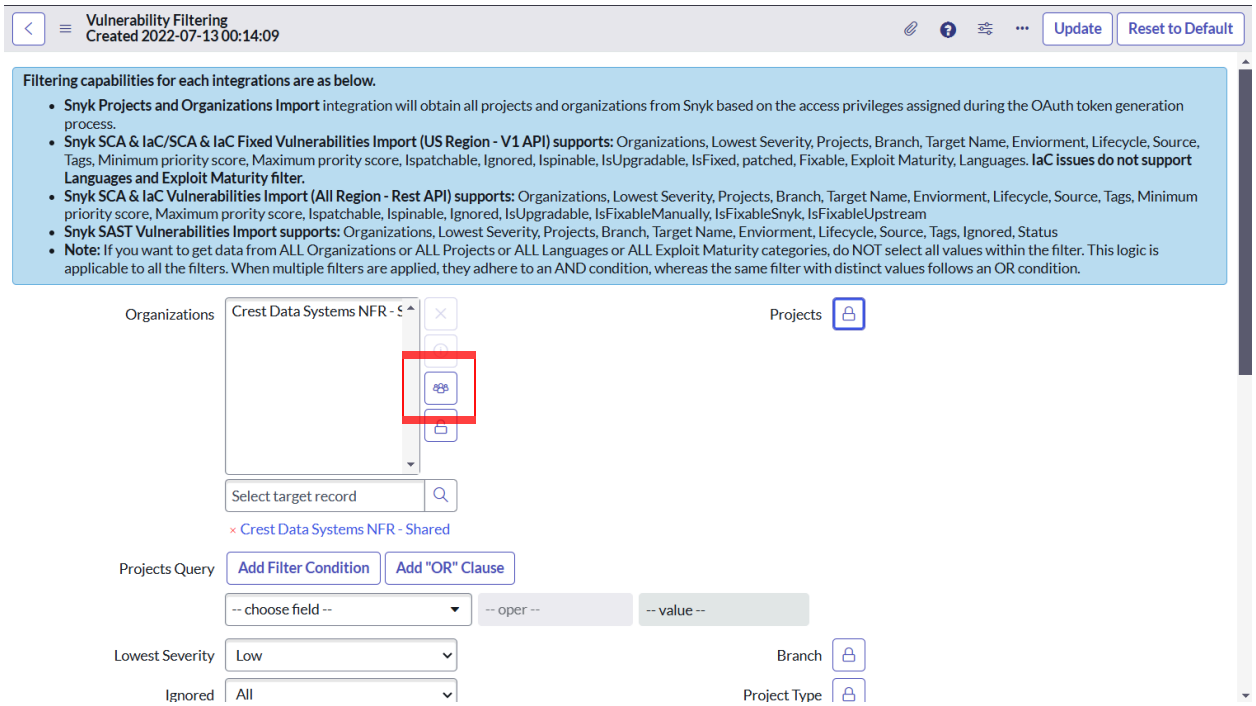
11. Select a value from the Target reference to filter the Vulnerable item ingestion.



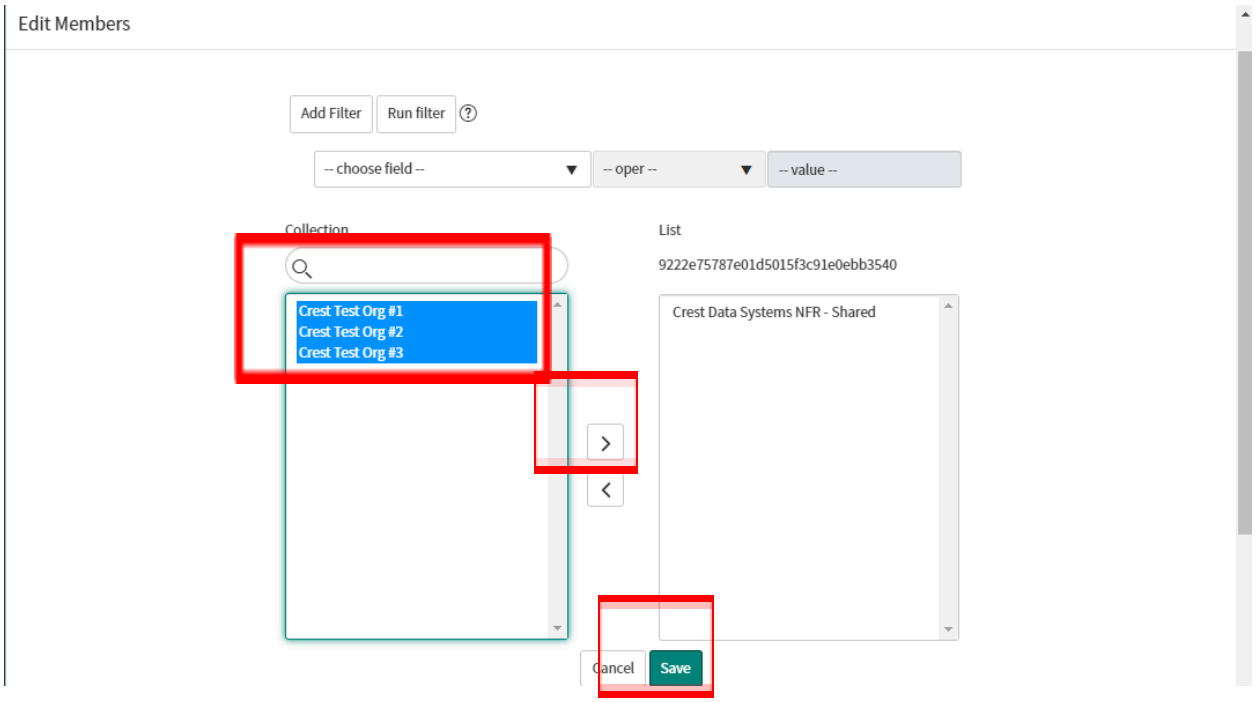
12. The selected organization and project will be visible to the user on the Vulnerability Filtering page as below.
13. If you want to fetch issues from all organizations and projects, leave the value empty. If selecting the projects filter, en**sure it does not exceed 1000 projects**. Refer to this link for more information about the issue API filtering.



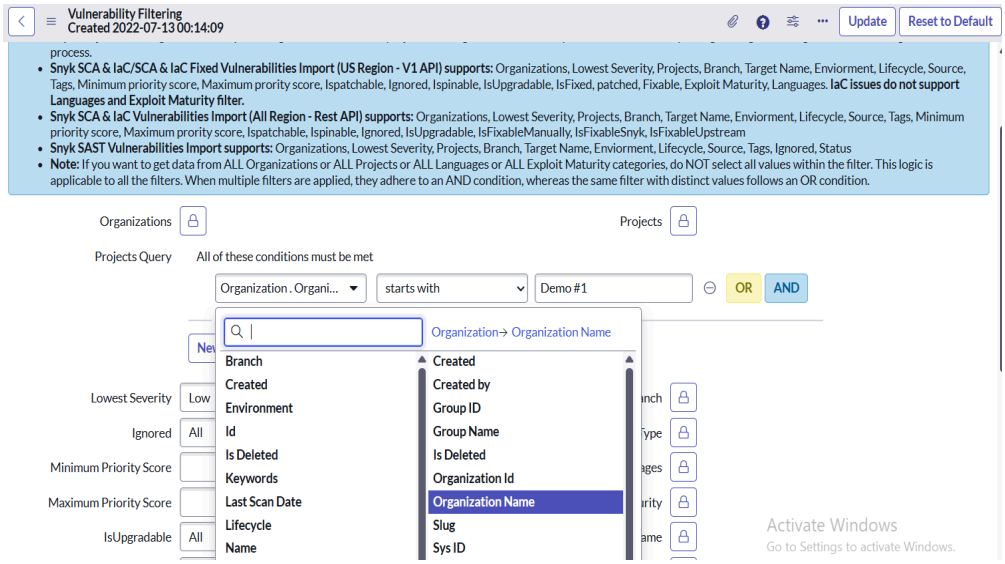
14. If users want to select multiple organizations or projects from the list, they must click the icon below.



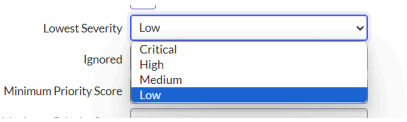
15. Users can select multiple values from the list on the left-hand side, click on ">" to move them into the selected list, and then click on the Save button, and vice versa.



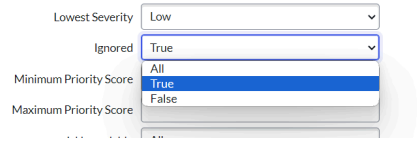
16. Users can use the Project Query filter to define conditions based on Organizations, Projects, Branch, Source, Target Name, Environment, Lifecycle, and Tags. Dot-walking to reference fields is also supported.



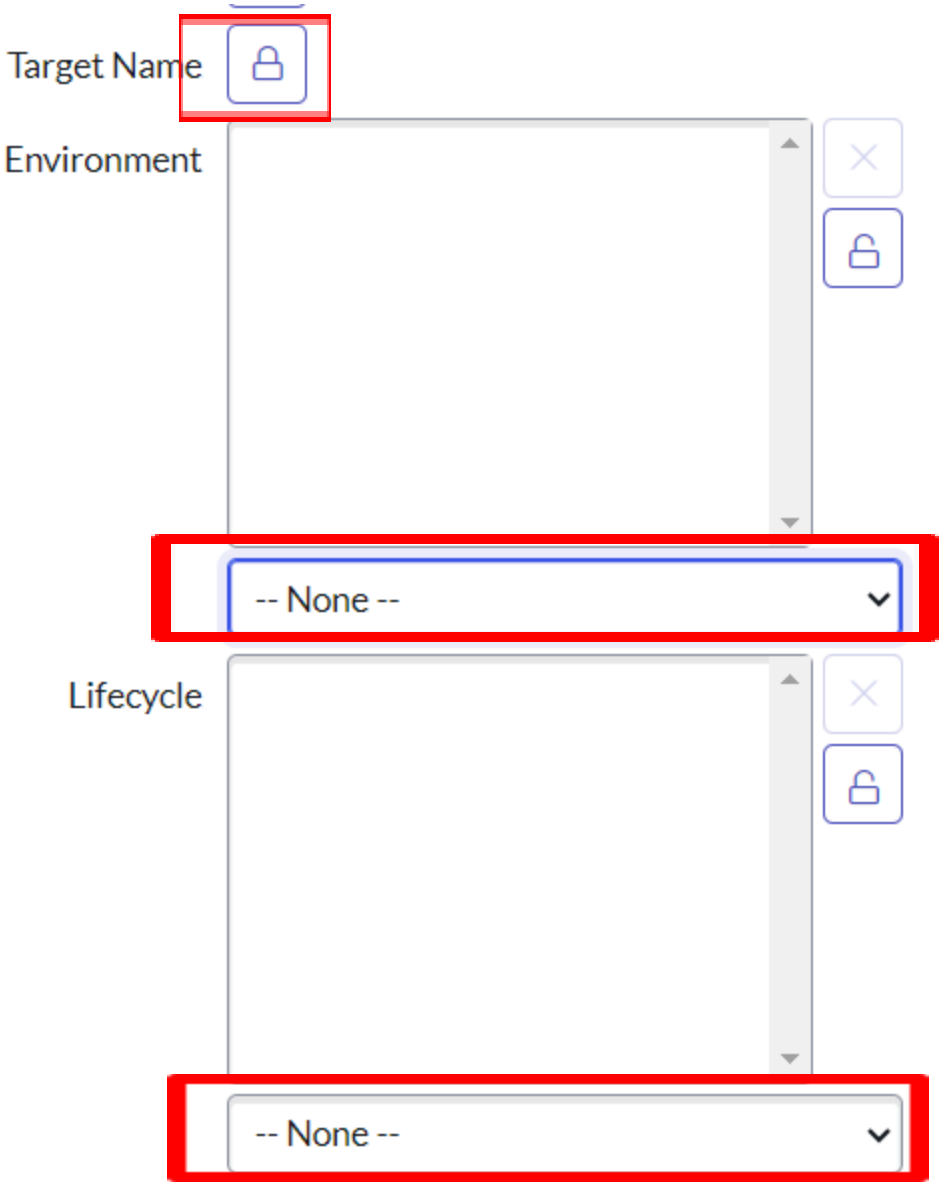
17. Users can select the severity from the dropdown of the lowest severity by clicking on the dropdown list.



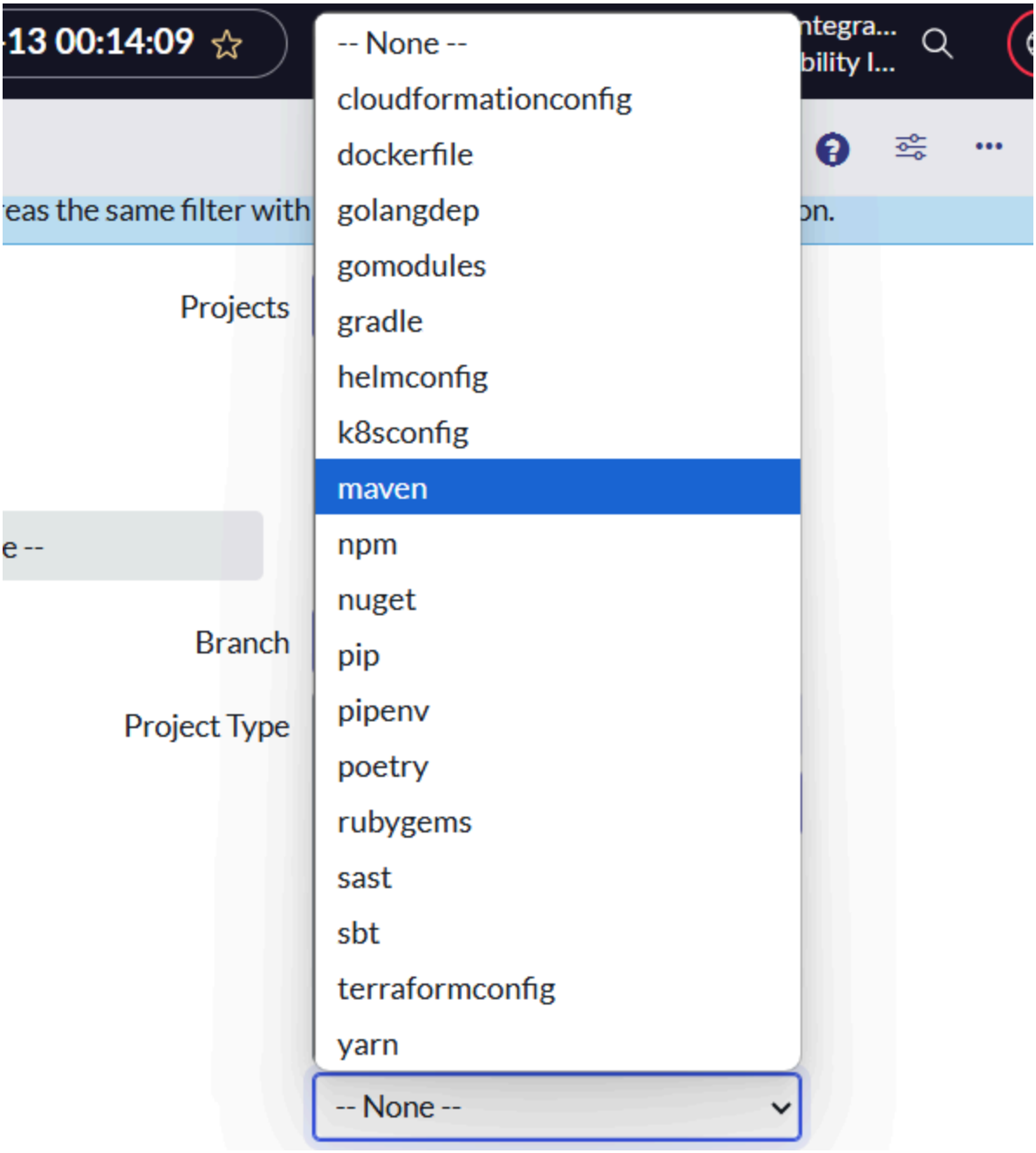
18. Users can select the Ignore, IsUpgradable, IsPatchable, Patched, Fixable, IsPinnable, and IsFixed values from the dropdown by clicking on the dropdown list.



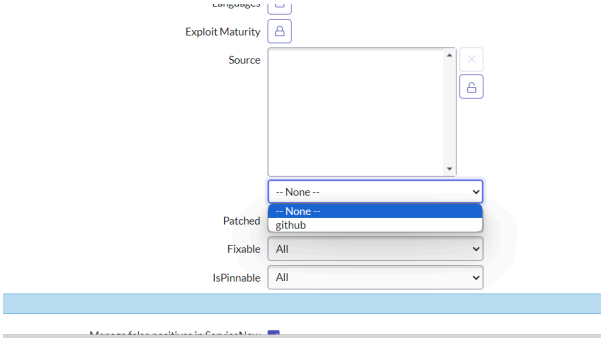
19. Users can select the Branch, Target Name, Environment, and Lifecycle value from the choices.



20. Users can select the Project Type value from the Project Type choices by clicking on the list.

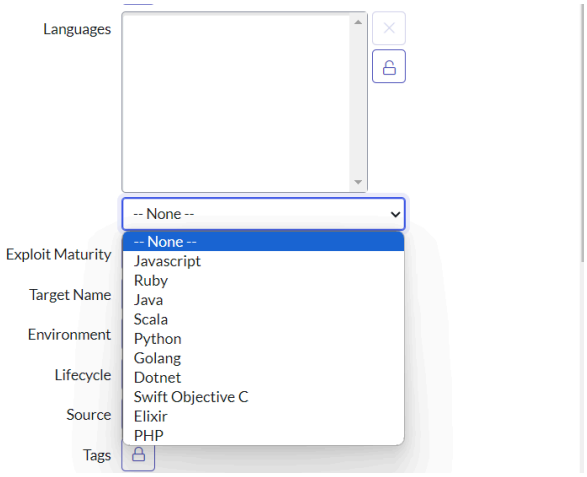


21. Users can select the Source value from the Source choices by clicking on the list.

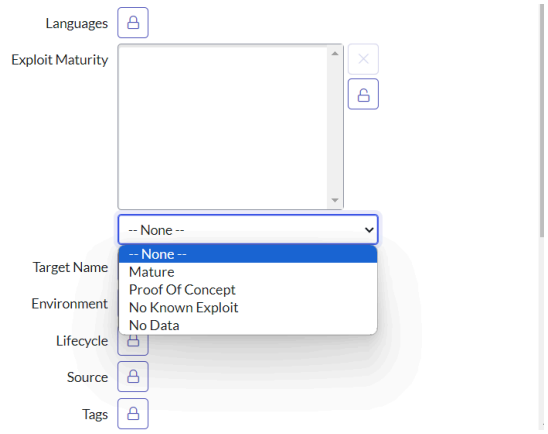


22. Users can provide values in Minimum Priority Score and Maximum Priority Score based on their requirements.
23. Users can select the Languages value from the Languages choices by clicking on the Choices list.

    Note: If the languages are not selected, the integration will fetch data for all the languages shown in the dropdown.

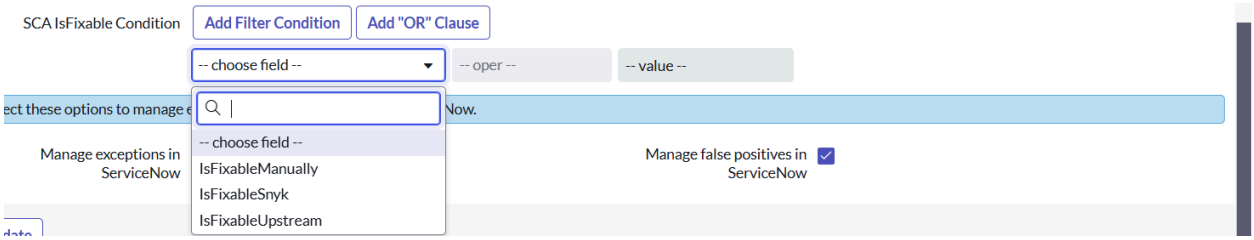


24. Users can select the Exploit Maturity value from the choices of Exploit Maturity by clicking on the Choices list.

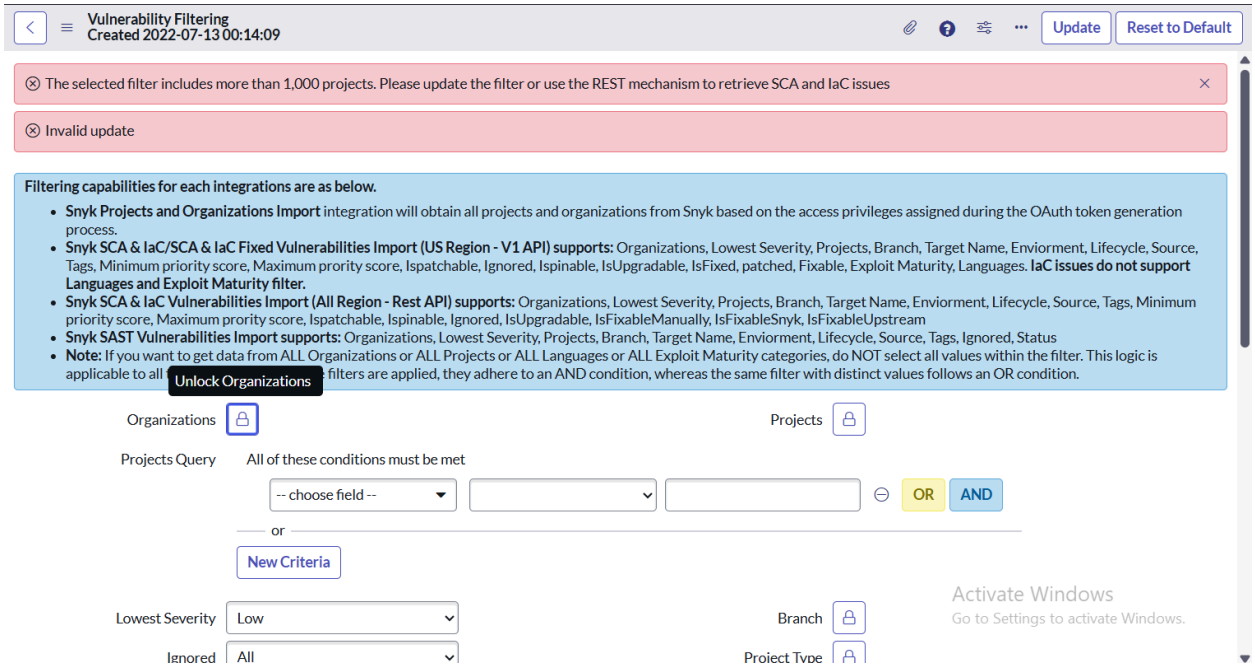


25. Users can select one of the isFixable types to filter when using the SCA REST Integration.

Note: Only the "is" operator is allowed.



26. If the Filtering has more than 1000 projects and User is using V1 API than Configuration will throw an error “The selected filter includes more than 1,000 projects. Please update the filter or use the REST mechanism to retrieve SCA and IaC issues.”



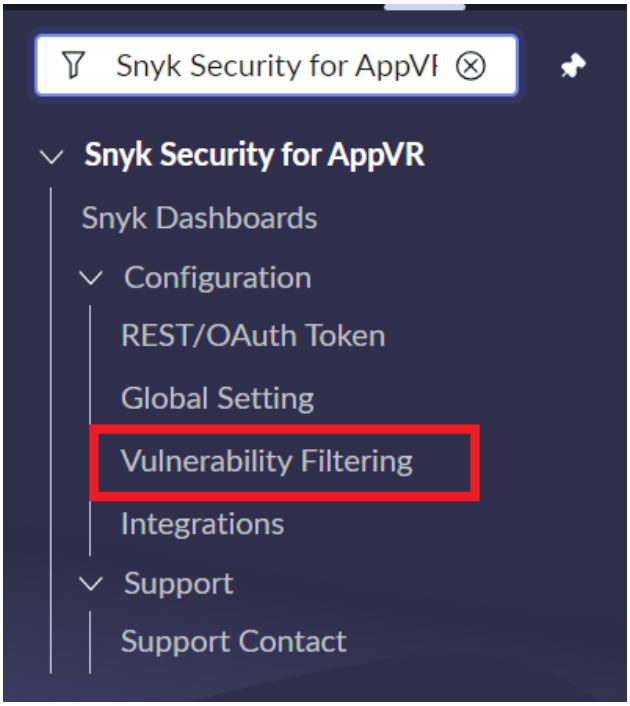
4.3. Managing Exceptions in ServiceNow

This section describes how to use "Managing in ServiceNow" to define the state of issues to be imported from Snyk.

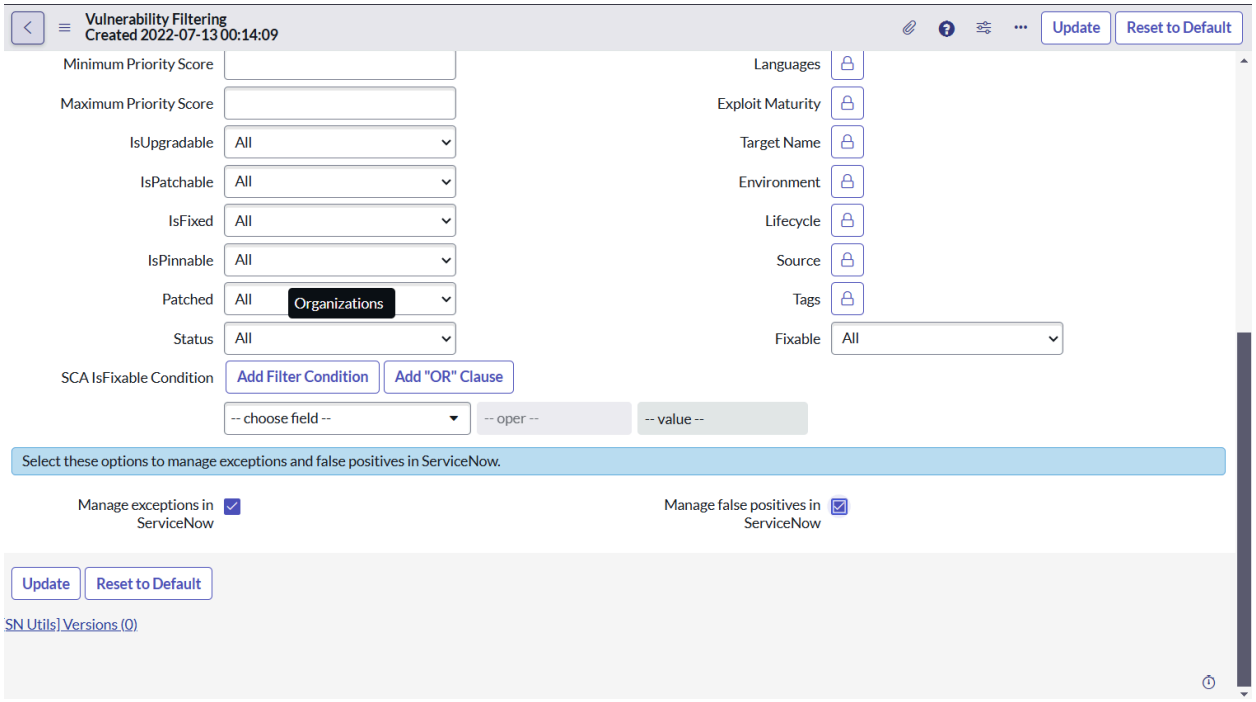
Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

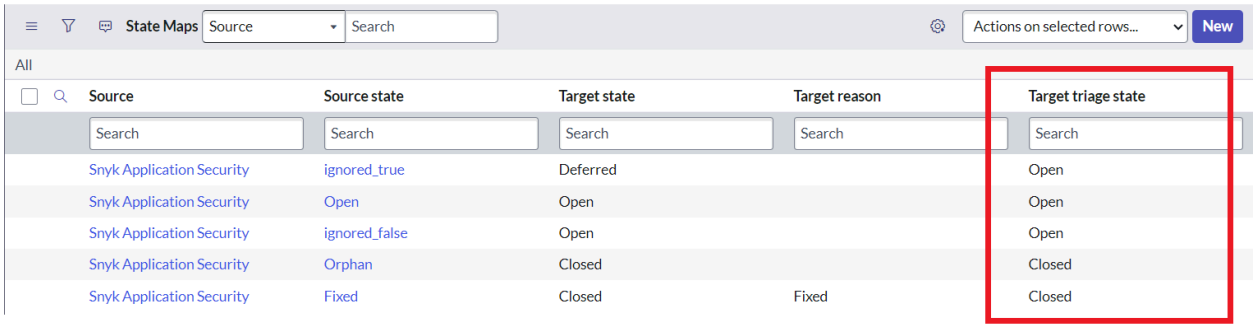
1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR" and select "Configuration."
3. Click on "Vulnerability Filtering."



4. Users can select "Manage exceptions in ServiceNow" and "Manage false positives in ServiceNow" by clicking on the checkbox and selecting the update button to update the vulnerability filtering form, as shown below.

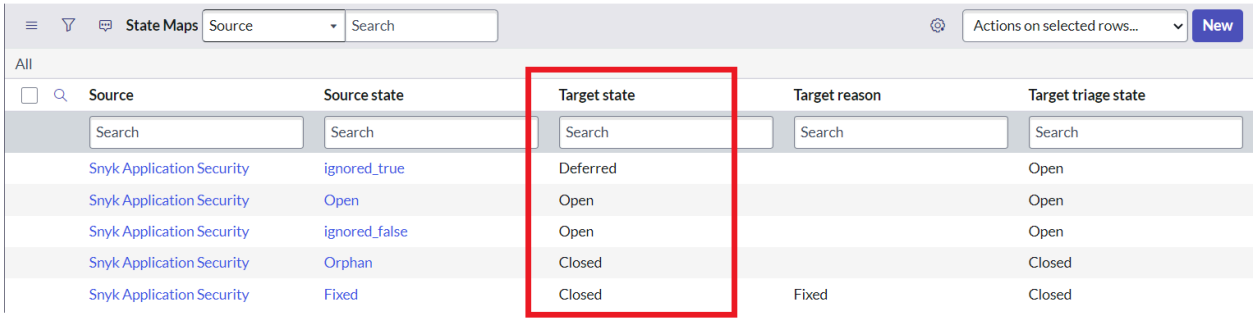


5. If the user selects the "Manage exceptions in ServiceNow" checkbox and imports an issue, then the AVIT created will have the state mapping for the "Target triage state" as shown below:



Source	Source state	Target state	Target reason	Target triage state
Search	Search	Search	Search	Search
Snyk Application Security	ignored_true	Deferred		Open
Snyk Application Security	Open	Open		Open
Snyk Application Security	ignored_false	Open		Open
Snyk Application Security	Orphan	Closed		Closed
Snyk Application Security	Fixed	Closed	Fixed	Closed

6. If the user does not select the "Manage exceptions in ServiceNow" checkbox and imports an issue, the AVIT created will have the state mapping for "Target state," as shown below.
7. **Approve requests in the Vulnerability:**
   a. "Manage exceptions in ServiceNow" and "Manage false positives" in ServiceNow. These options are available under Vulnerability Filtering. If the checkboxes are selected, buttons will be visible on the Vulnerability Item form to initiate the action. Once clicked on the button to run the action, a request is sent for approval to the user/group defined in the approval workflow.
   b. Please review the link for more information - https://docs.servicenow.com/bundle/washingtondc-security-management/page/product/vulnerability-response/task/vr-ws-approve-requests.html.
8. Note: The functional details are mentioned in sections 6.3.3 and 6.3.4



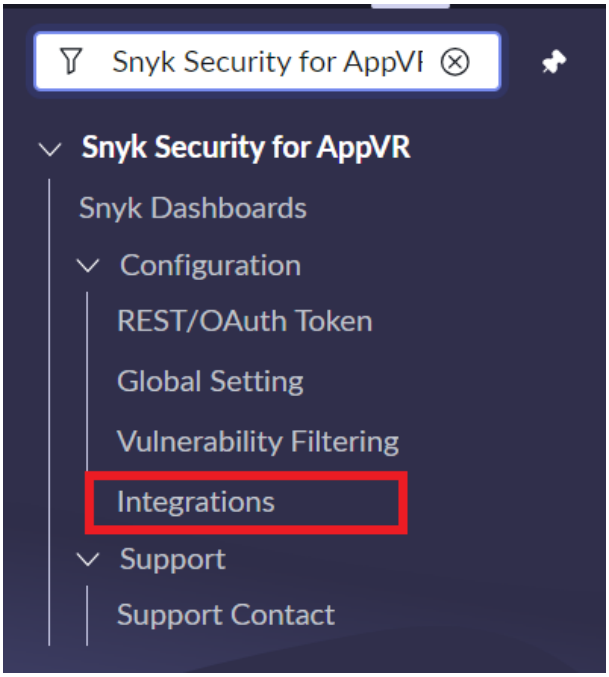
Source	Source state	Target state	Target reason	Target triage state
Search	Search	Search	Search	Search
Snyk Application Security	ignored_true	Deferred		Open
Snyk Application Security	Open	Open		Open
Snyk Application Security	ignored_false	Open		Open
Snyk Application Security	Orphan	Closed		Closed
Snyk Application Security	Fixed	Closed	Fixed	Closed

4.4. Fetch SAST Issues from the Snyk platform.

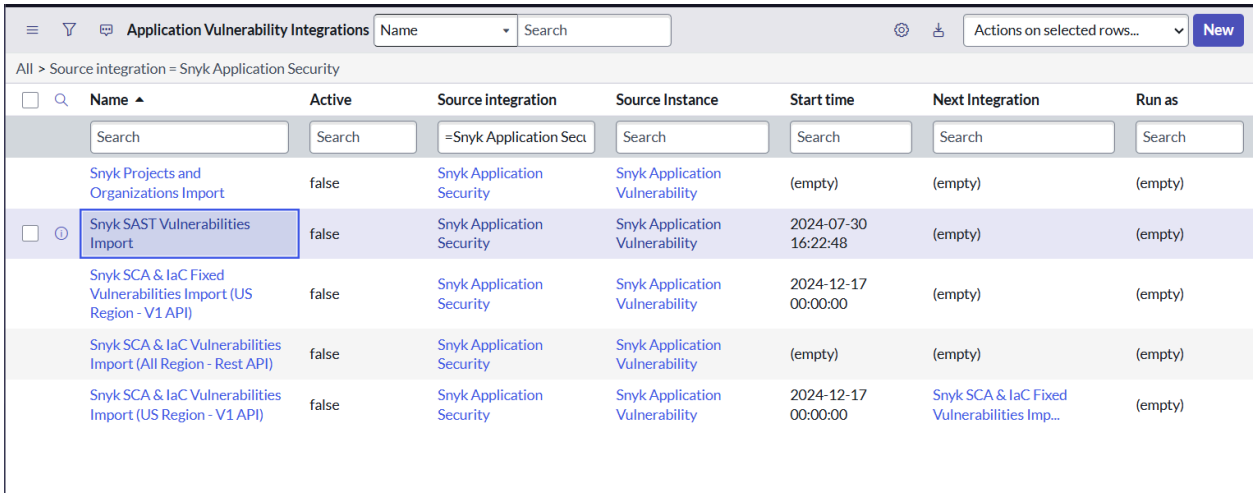
Note: This integration is standard for fetching SAST data from any region, i.e., AU, EU, or US.
"Snyk Security for AppVR" provides the functionality to fetch SAST Issues and their details from Snyk and populate them as Vulnerability, Application Vulnerable Item, and Application Scan Summary in ServiceNow.
Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

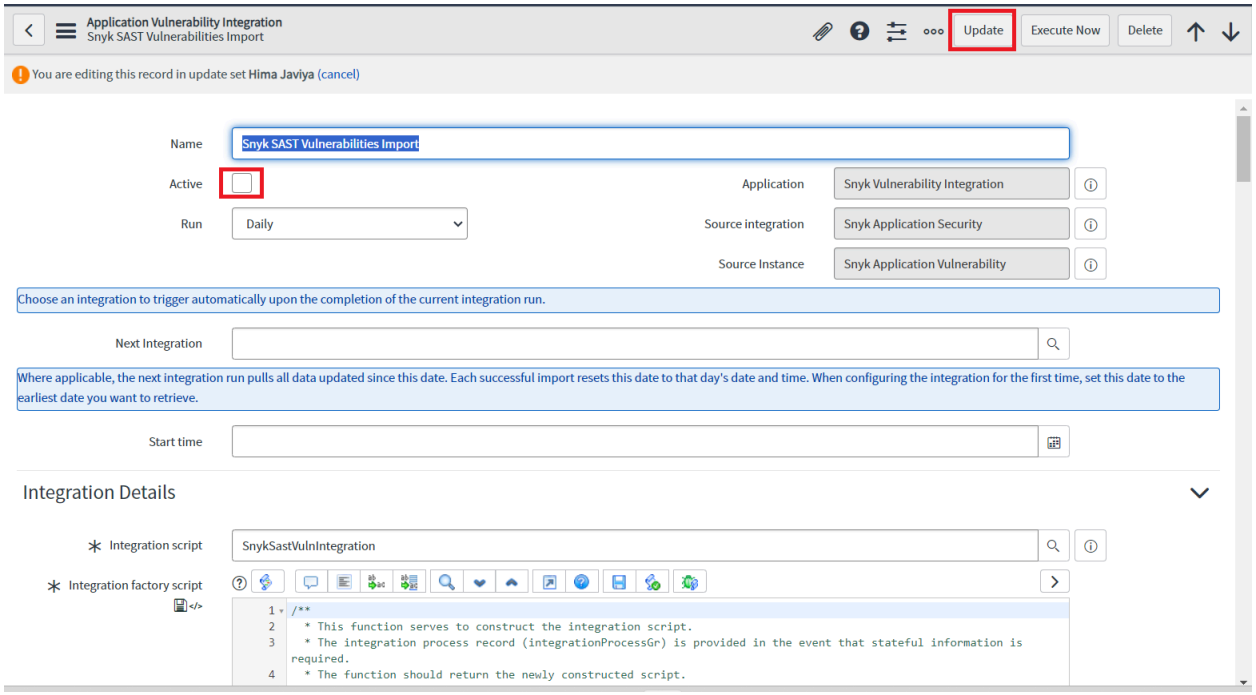
1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR," and under it, select "Configuration."
3. Click on "Integrations."



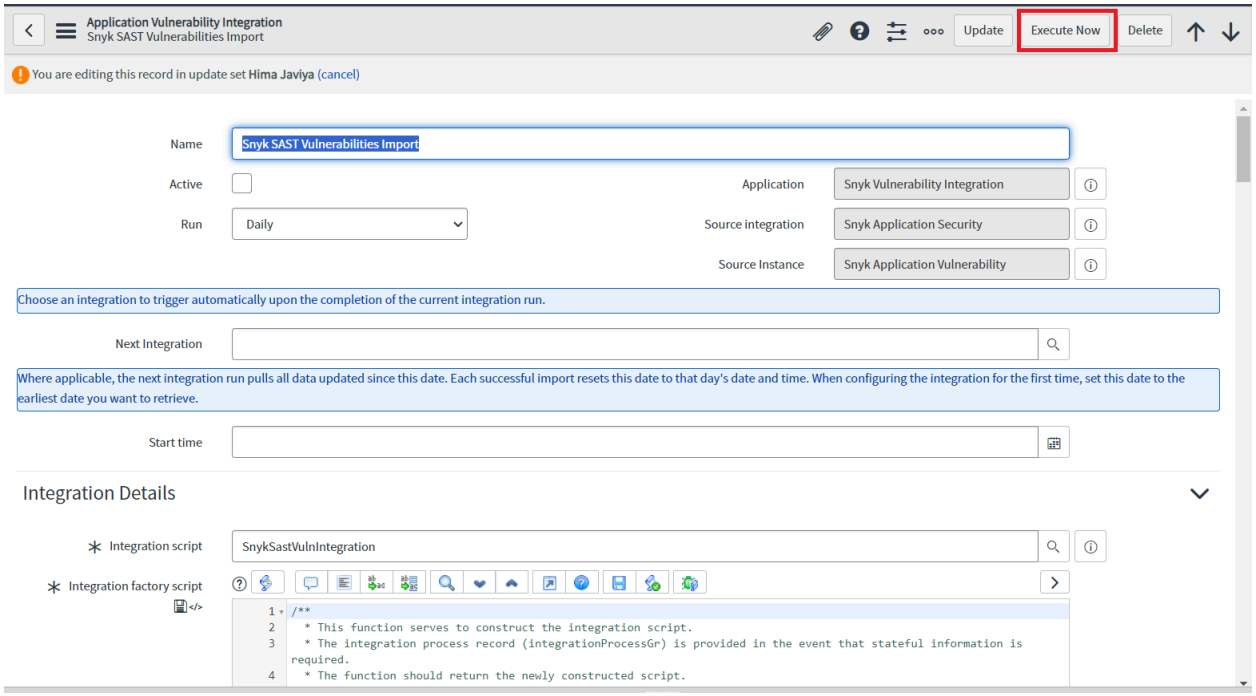
4. Select Integration with the name "Snyk SAST Vulnerabilities Import" and Source Instance value as default provided integration instance.



5. Activate the checkbox "Active." Click on the button "Update."
6. You must change the start time system property if you want to change the start time. By default, it will fetch all the code issues from Snyk.

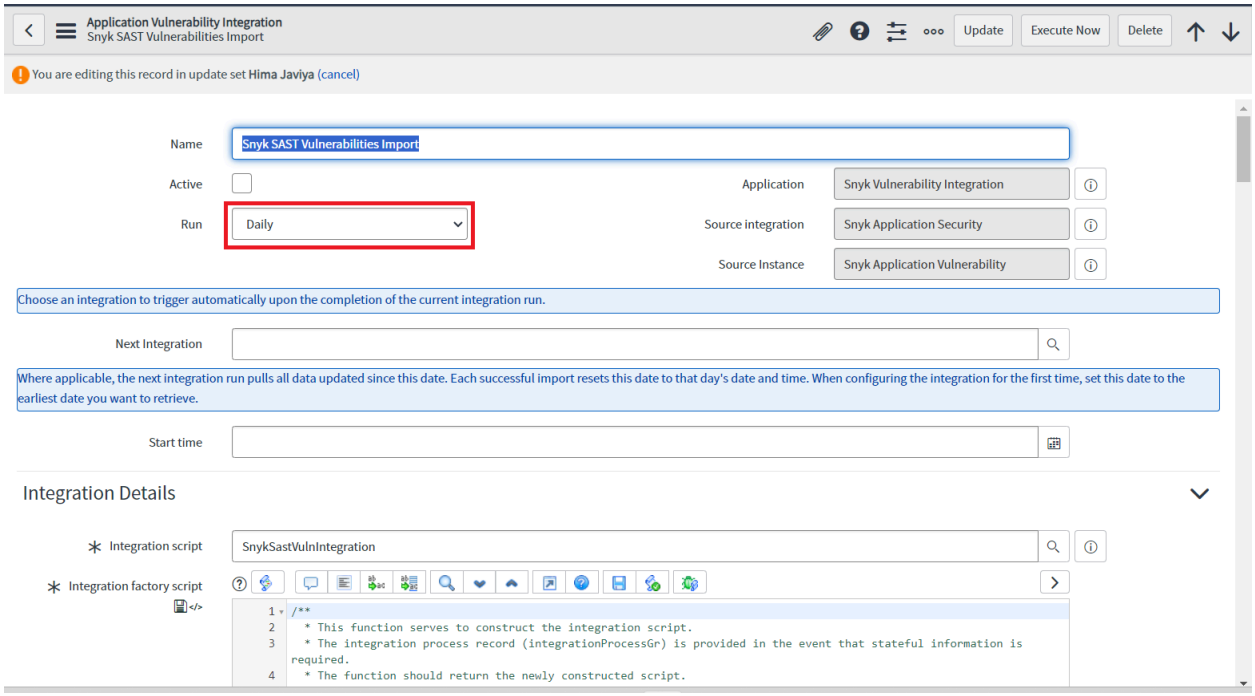


7. Open the Snyk SAST Integration record. To fetch issues currently, click on the "Execute Now" button.



8. To fetch issues within a specific interval, select the relevant option from the Run dropdown, set the time, and click the "Update" button.

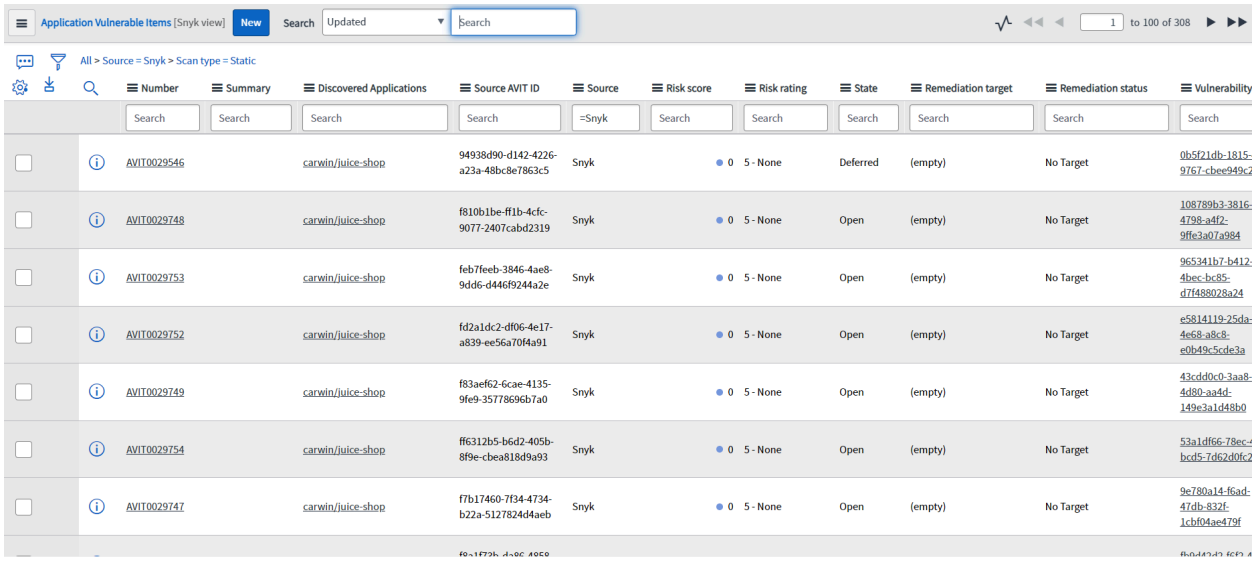
Note: The default time is 4:00 for SCA integration, which is 2 hours later than the Project and Orgs integration time so that tokens can be generated without token conflicts.



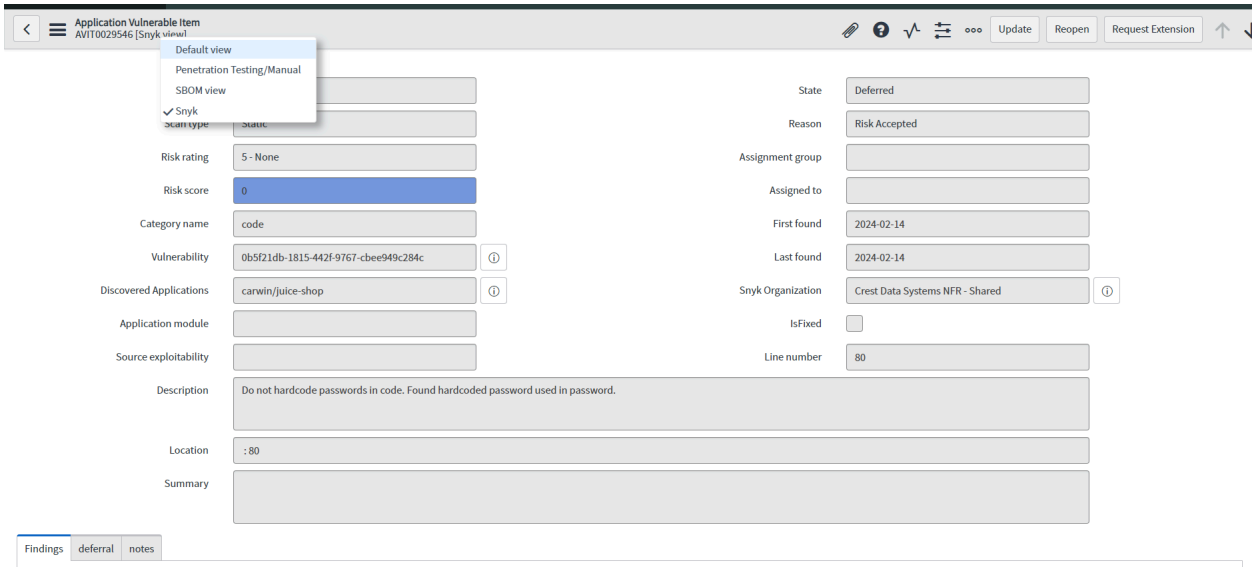
9. To view collected issues, navigate to "Application Vulnerability Response," under it click on "Vulnerable Items" and under it select "All."


servicenow
All
Application vulnerability
ALL RESULTS
Application Vulnerability Resp...
My Approvals
Remediation Tasks
Active
Assigned to Me
Assigned to My Groups
All
Vulnerable Items
Active
Assigned to Me
Assigned to My Groups
Missed Remediation Commi...
Multiple Deferrals
Unassigned
All
Penetration Test Assessmen...
Active
Assigned to Me

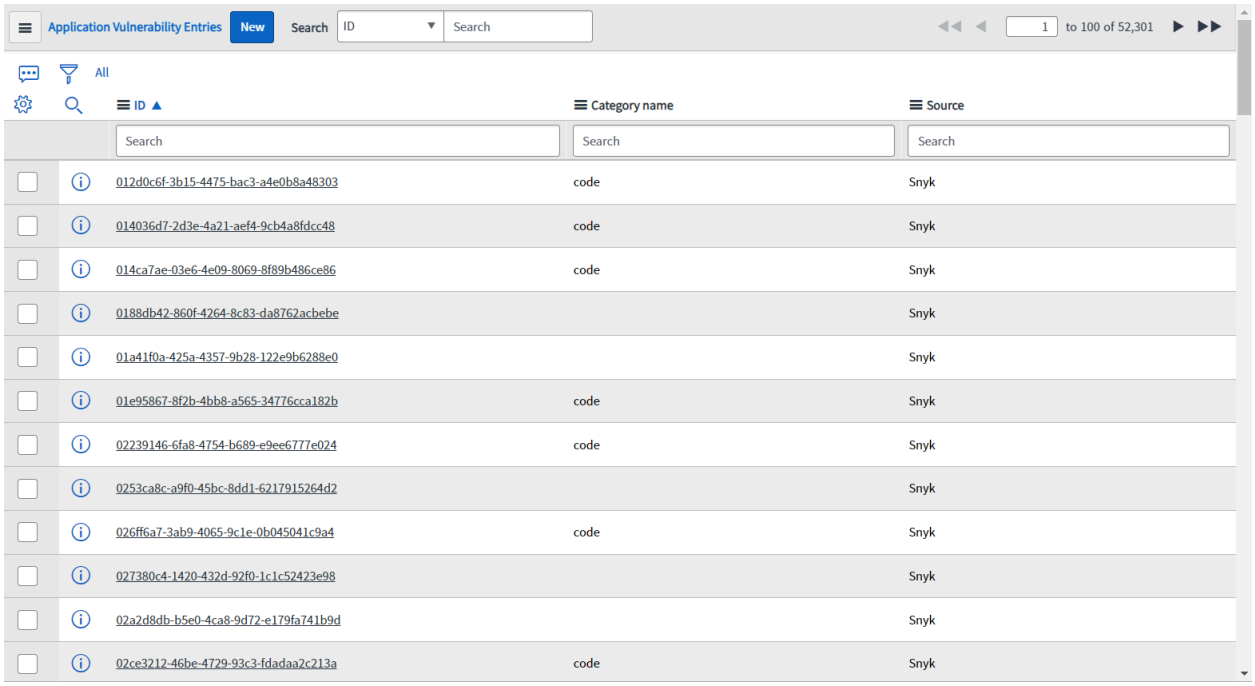
10. Users will have to provide the filter as "Source" "is" "Snyk" AND "Scan Type" "is" "Static." Then click "Run" to view all the SAST issues retrieved from Snyk.



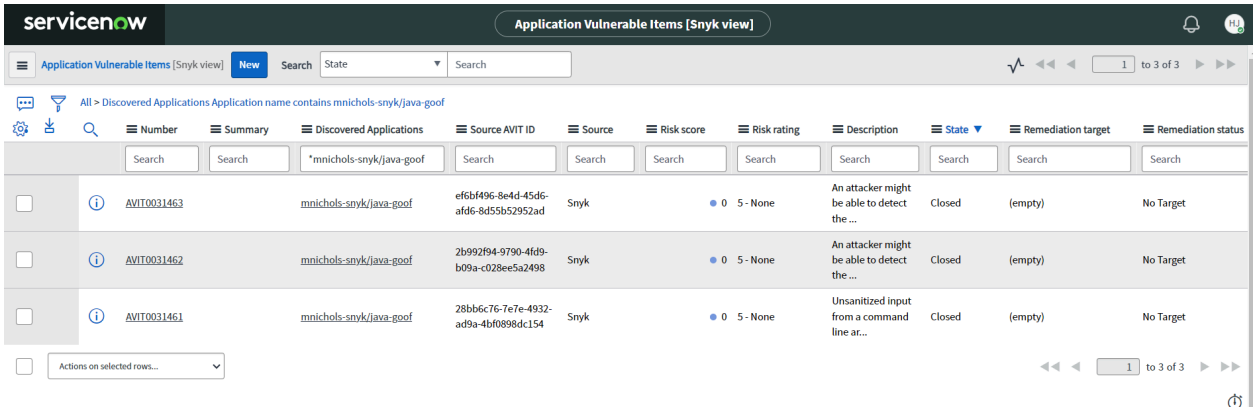
11. Change the view to "Snyk" to view the Snyk mapping fields in the AVIT table.



12. Third-party vulnerabilities will be visible in the list view of the "Application Vulnerability Entries (sn_vul_app_vul_entry)."
Note: Third-party vulnerability will only contain CWE as part of the SAST issue.



13. If a project is deleted or deactivated after the AVIT is created, the AVIT state will be closed with a proper note in the Description in the subsequent ingestion of issues.



14. If the user marks an AVIT as "Mark as False Positive" or "Request Exception," the AVIT state will be set to "In Review." Once the request is approved, the "Additional comment," "Until date," "Reason," and "Additional comment" in the request exception added by the user will be added to the Snyk platform user interface. The AVIT state will be set to "Closed" after an approver approves the request.

Note: The "Mark as False Positive" and "Request Exception" buttons will only be visible when the "Manage Exception in ServiceNow" & "Manage False Positive in ServiceNow" flag are set to "true" in the Vulnerability Filtering section. Selecting "Mark as False Positive" will permanently ignore the issue in Snyk.

Once the AVIT is "Approved" and the state is changed, the user can see the "Additional information" added to the issue on the Snyk platform. Users must click on the "Source link" in the AVIT's Findings, redirecting them to the Snyk platform on the Issues page. Then, the user needs to add an "ignored" parameter in the filter.

Users will be able to see the issue with the comment. The comment will include the AVIT Number with the reason added from the ServiceNow side.
AVIT closed on ServiceNow due to project inactive/deleted will not close issue on Snyk Platform.

4.5. Fetch SCA & IaC Issues from the Snyk platform(Only for the US region)

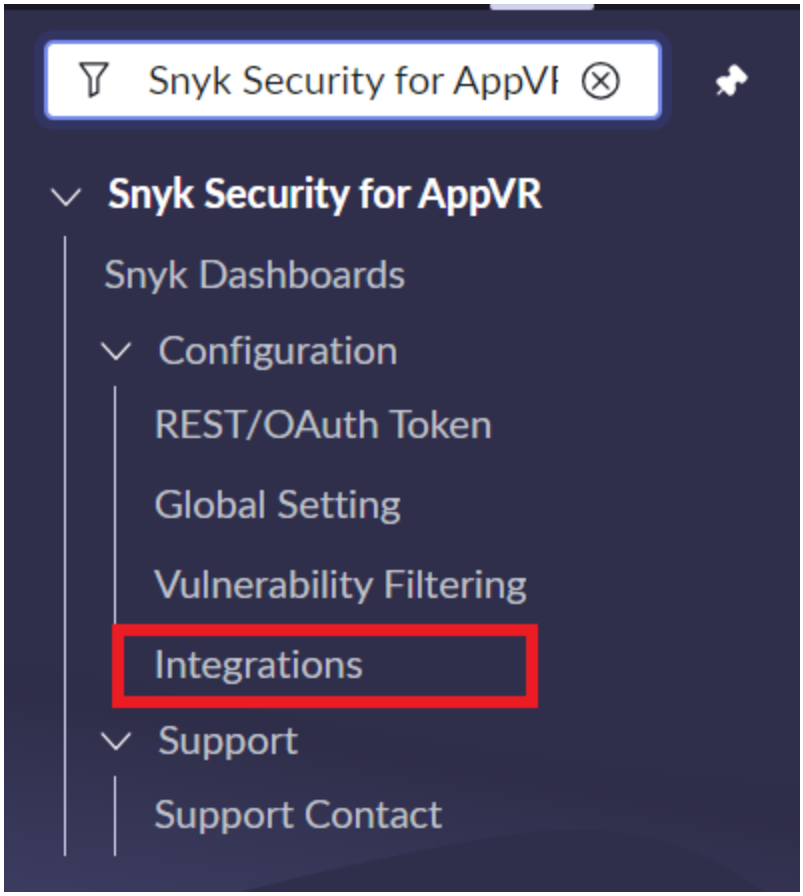
"Snyk Security for AppVR" provides the functionality to fetch Issues and their details from Snyk and populate them as Vulnerability, Application Vulnerable Item, Application Scan Summary, and Package in ServiceNow.

Important Note: Customers hosted in the `us.snyk.io` (AWS) region MUST use the REST APIs.

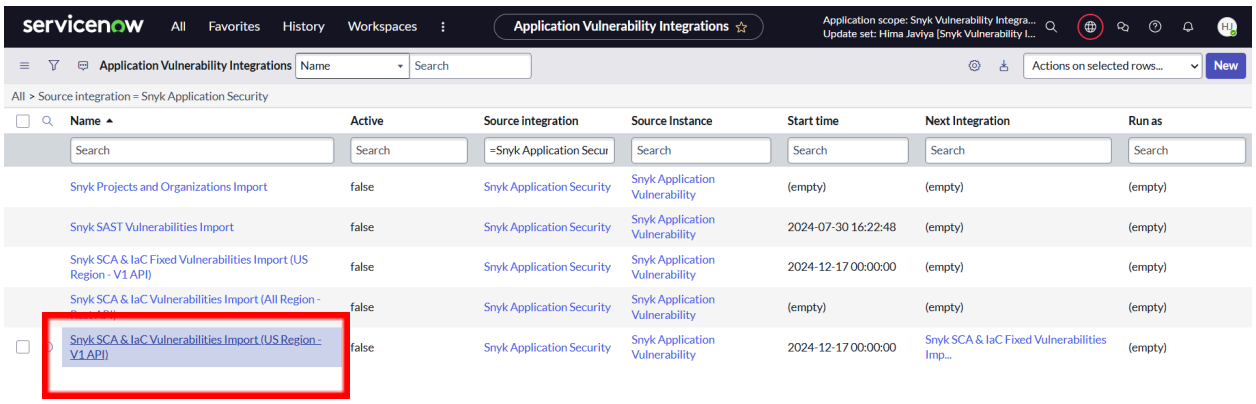
Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR," and under it, select "Configuration."
3. Click on "Integrations."

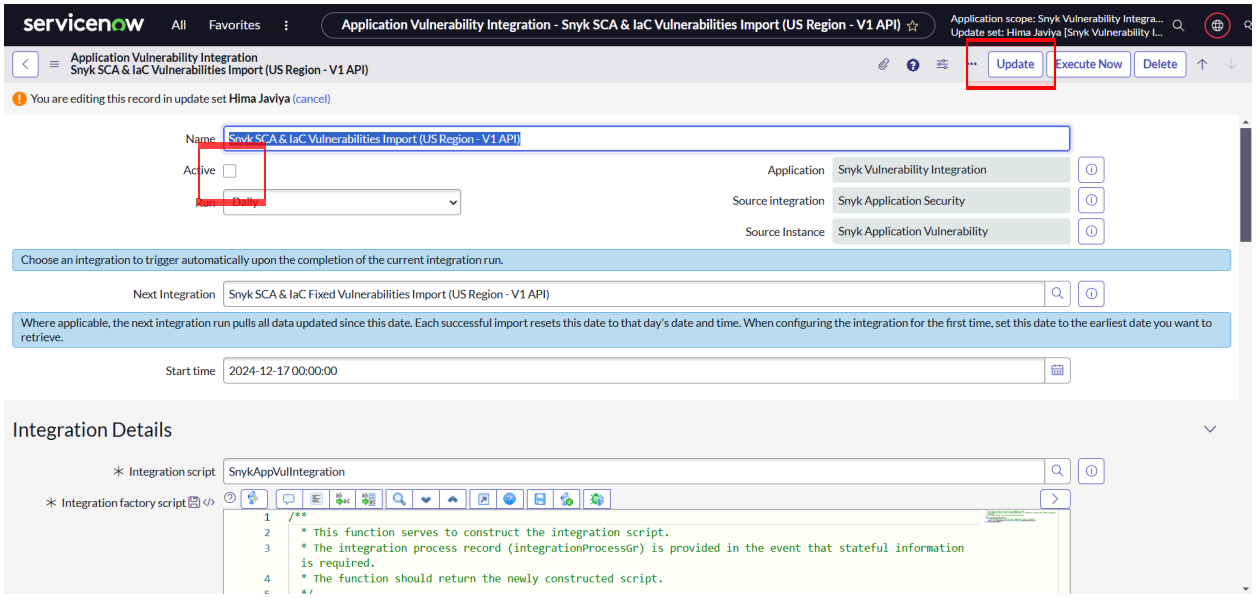


4. Select Integration with the name "Snyk SCA & IaC Vulnerabilities Import(US Region - V1 API)" and Source Instance value as default provided integration instance.

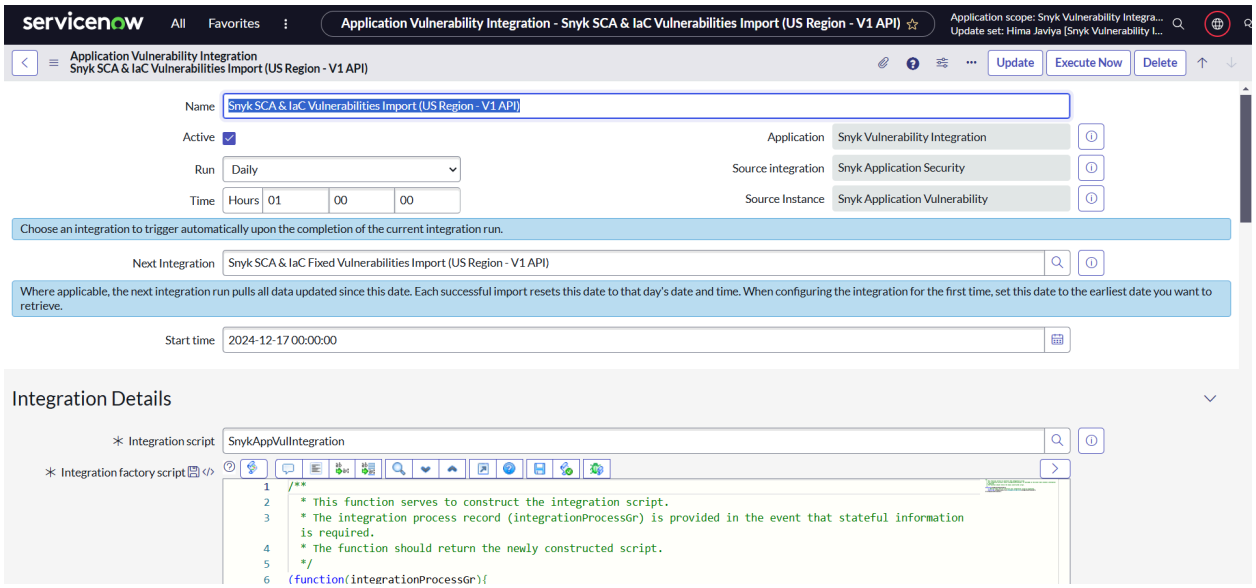


5. Activate the checkbox "**Active**." Click on the button **"Update."**

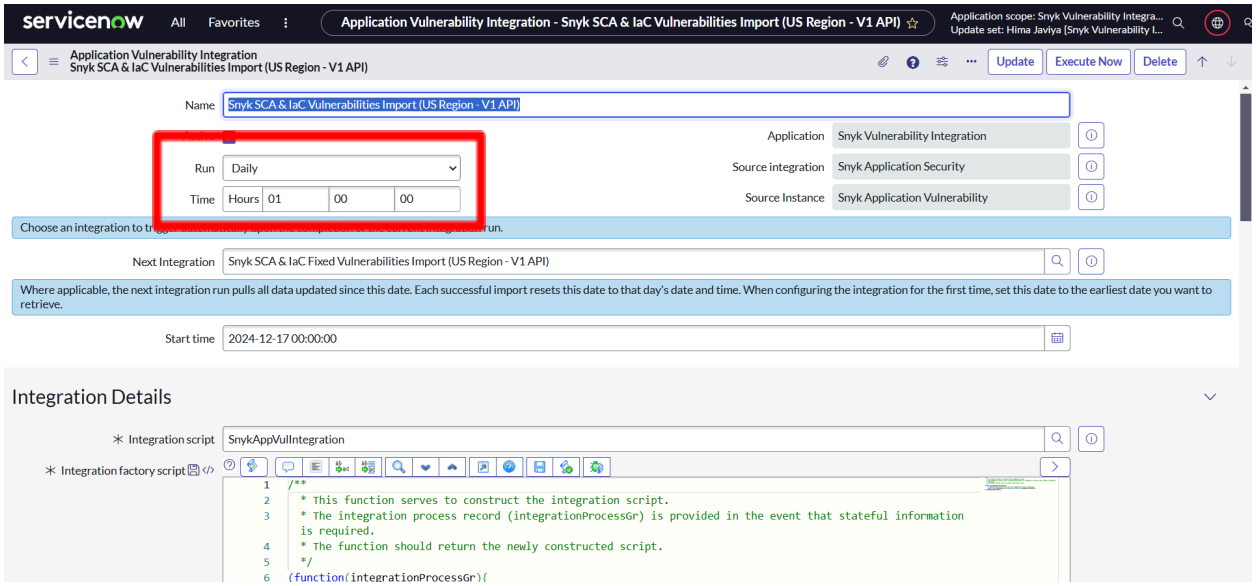
6. You must change the start time system property to change the start time. By default, it will take 90 days from the current time if the integration start time is blank.



7. Open the Snyk Integration record. To Fetch issues immediately, click on the "Execute Now" button.



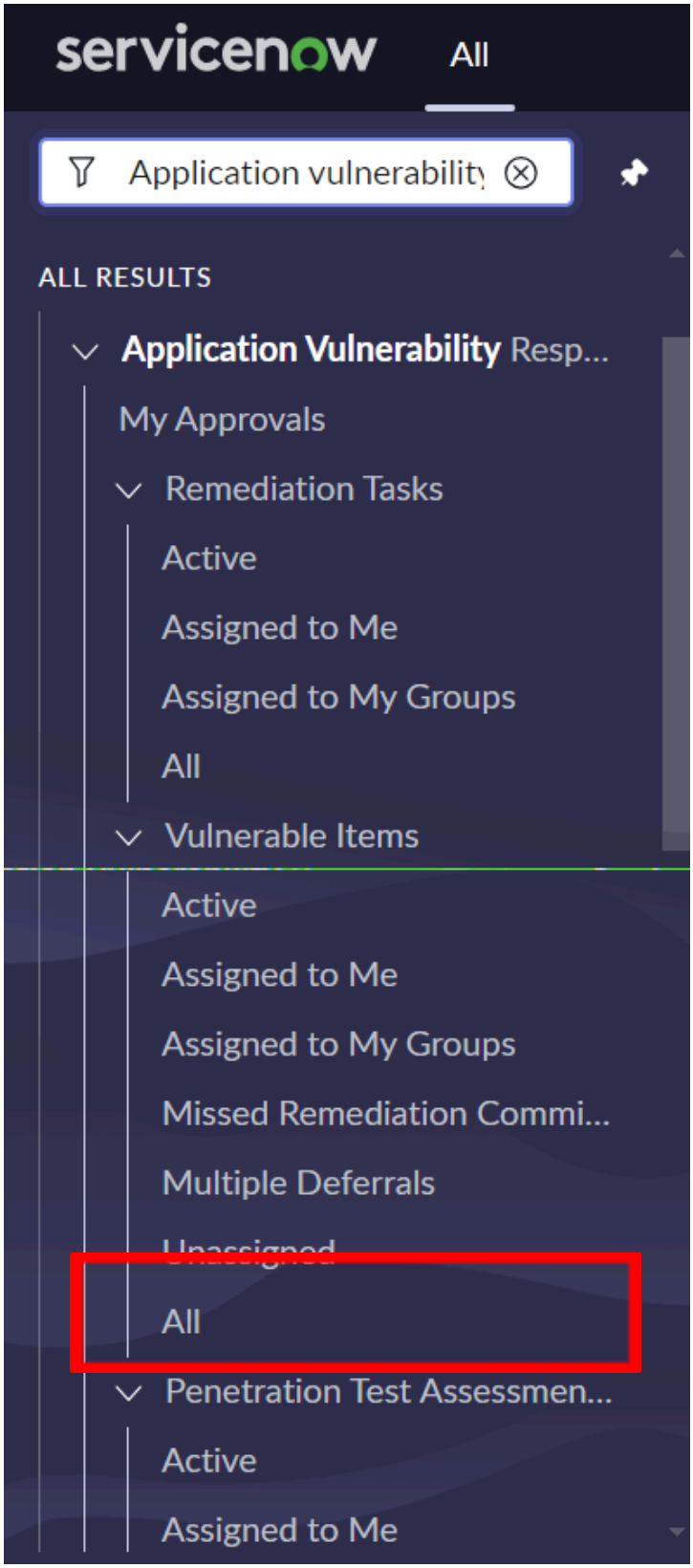
8. To fetch issues according to a scheduled time interval, select the relevant option from the Run dropdown, set the time, and click the "Update" button.



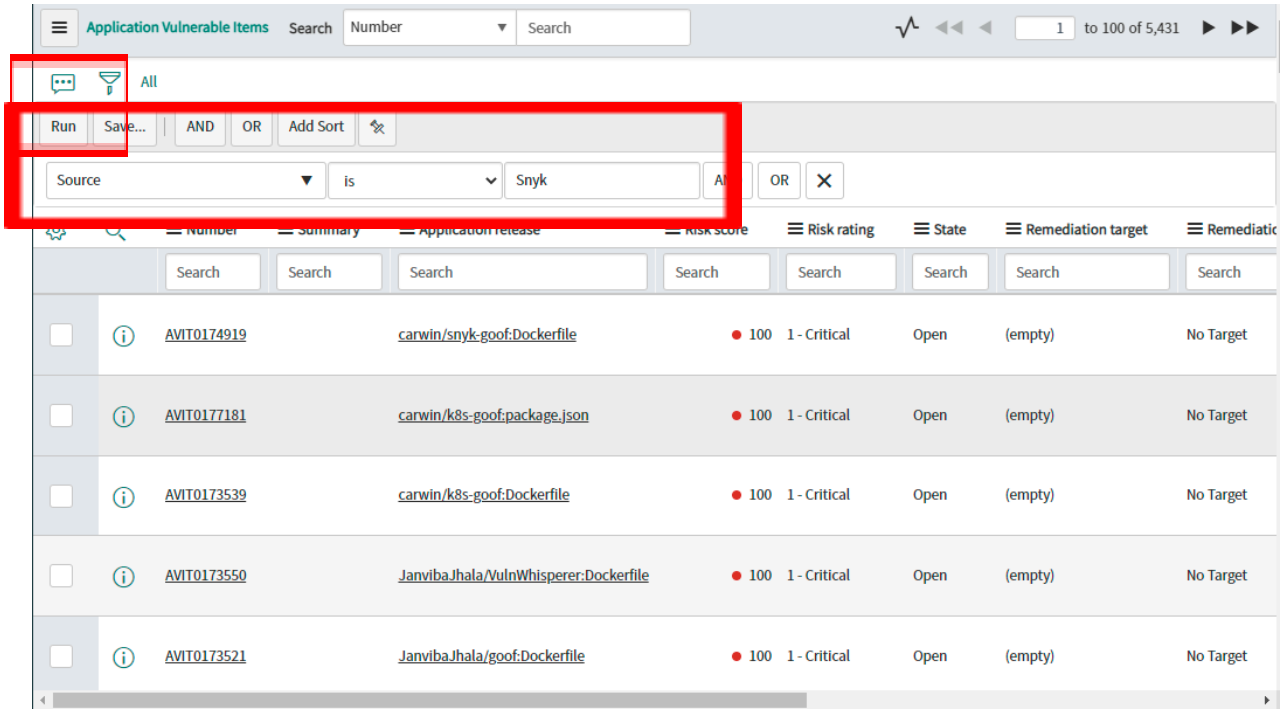
9. "Snyk SCA & IaC Fixed Vulnerabilities Import(US Region - V1 API)" by default will be provided in the subsequent Integration for "Snyk SCA & IaC Vulnerabilities Import(US Region - V1 API)," which means it will trigger automatically once the "Snyk SCA & IaC Vulnerabilities Import(US Region - V1 API)" finishes its execution.

   Note: The default time for SCA integration is 1:00, which is one hour later than the Project and Orgs integration time so that the token can be generated without any token conflicts.

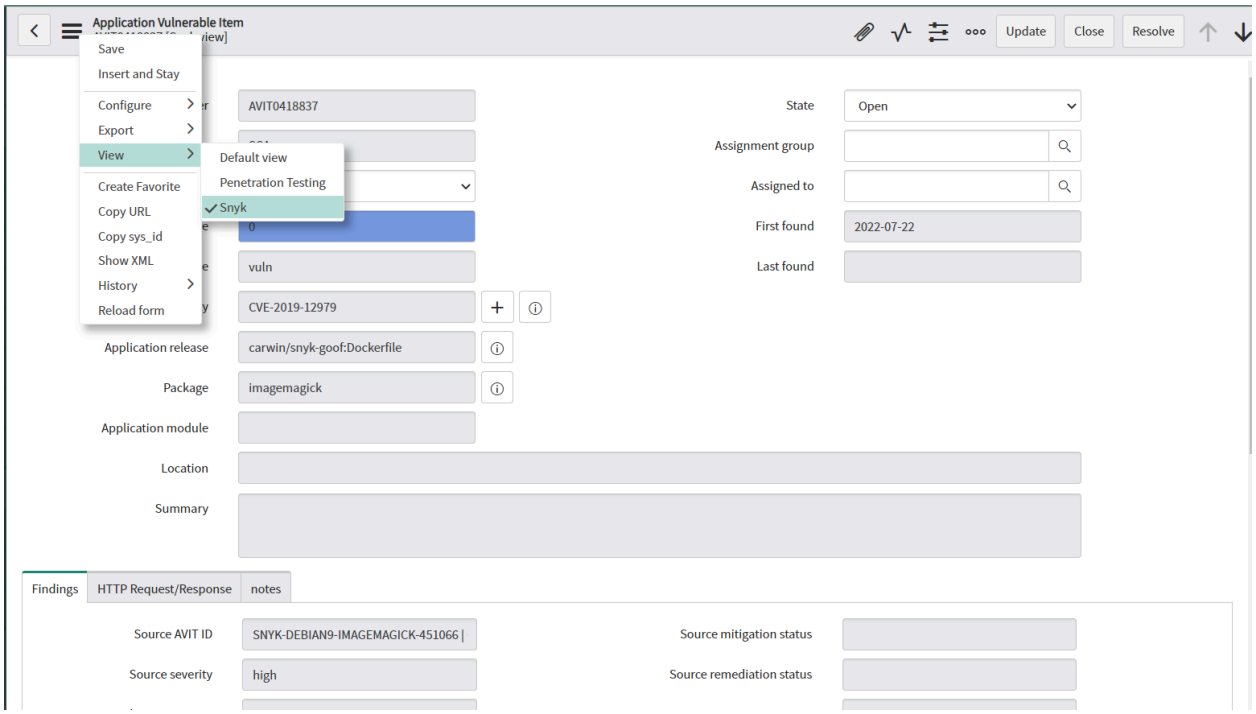
10. To view collected issues, navigate to "Application Vulnerability Response." Under it, click "Vulnerable Items," and under it, select "All."


servicenow
All
Application vulnerability
ALL RESULTS
Application Vulnerability Resp...
My Approvals
Remediation Tasks
Active
Assigned to Me
Assigned to My Groups
All
Vulnerable Items
Active
Assigned to Me
Assigned to My Groups
Missed Remediation Commi...
Multiple Deferrals
All
Penetration Test Assessmen...
Active
Assigned to Me

11. Users will have to provide the filter as "Source" "is" "Snyk" and then click on "Run" to view all the issues that are fetched from the Snyk.

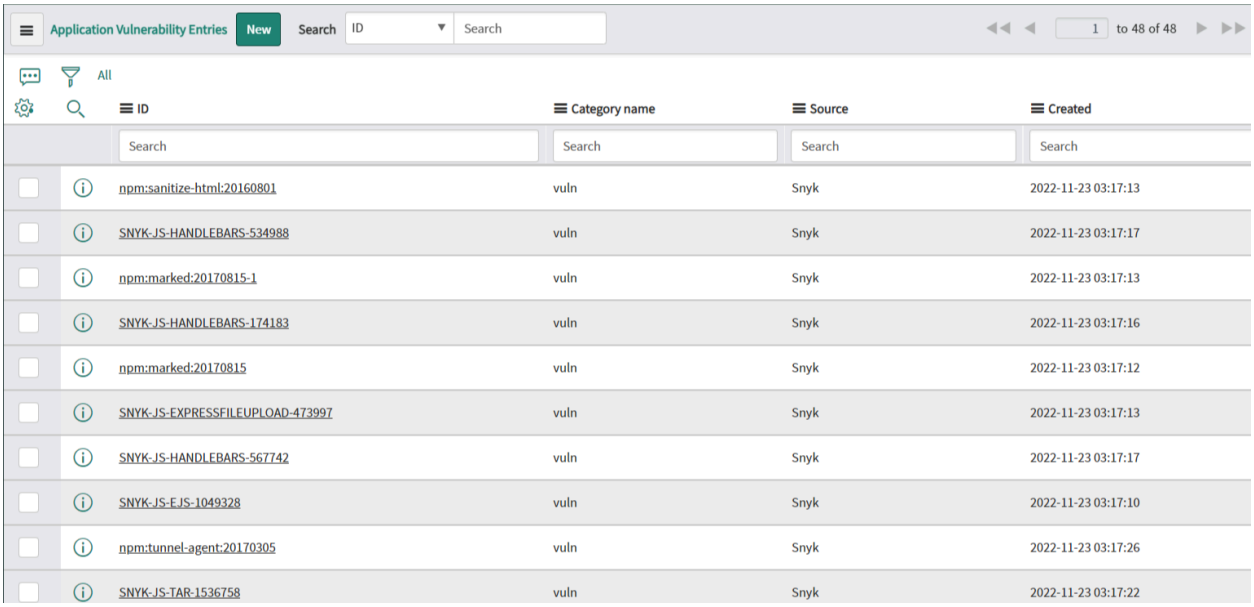


12. Change the view to "Snyk" to view the "Snyk Priority Score" in the AVIT table.



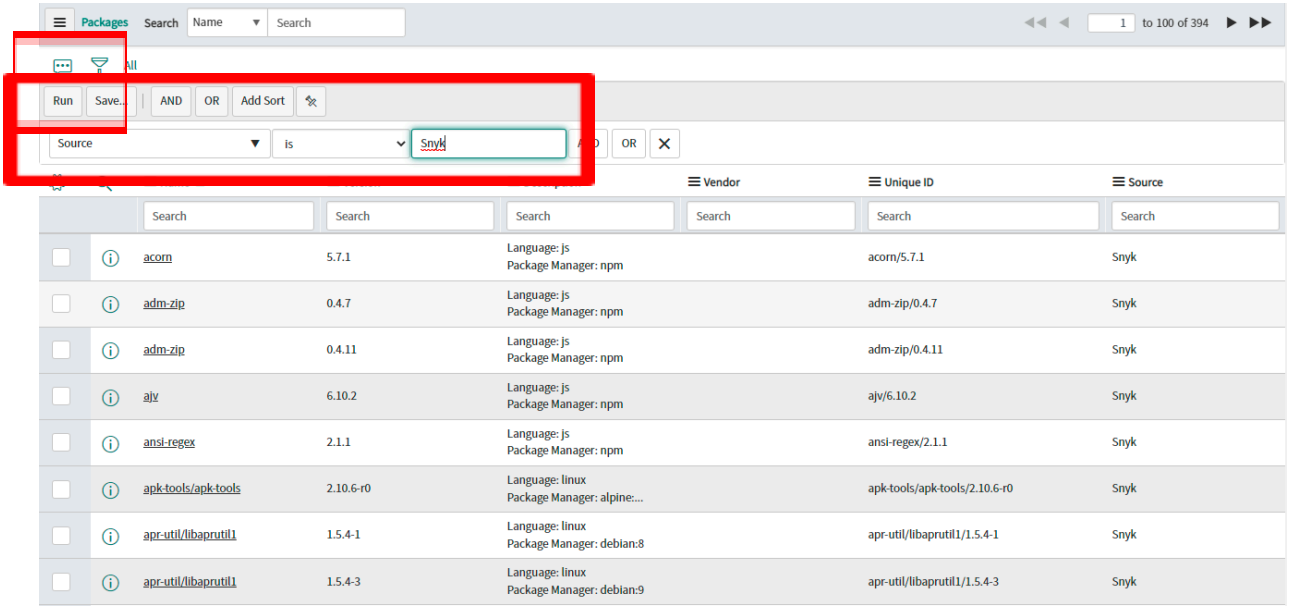
13. Third-party vulnerabilities will be visible in the list view of the "Application Vulnerability Entries (sn_vul_app_vul_entry)."

Note: A third-party vulnerability will only be created when the Snyk issue does not contain CVEs. IaC issues will always create a third-party vulnerability.

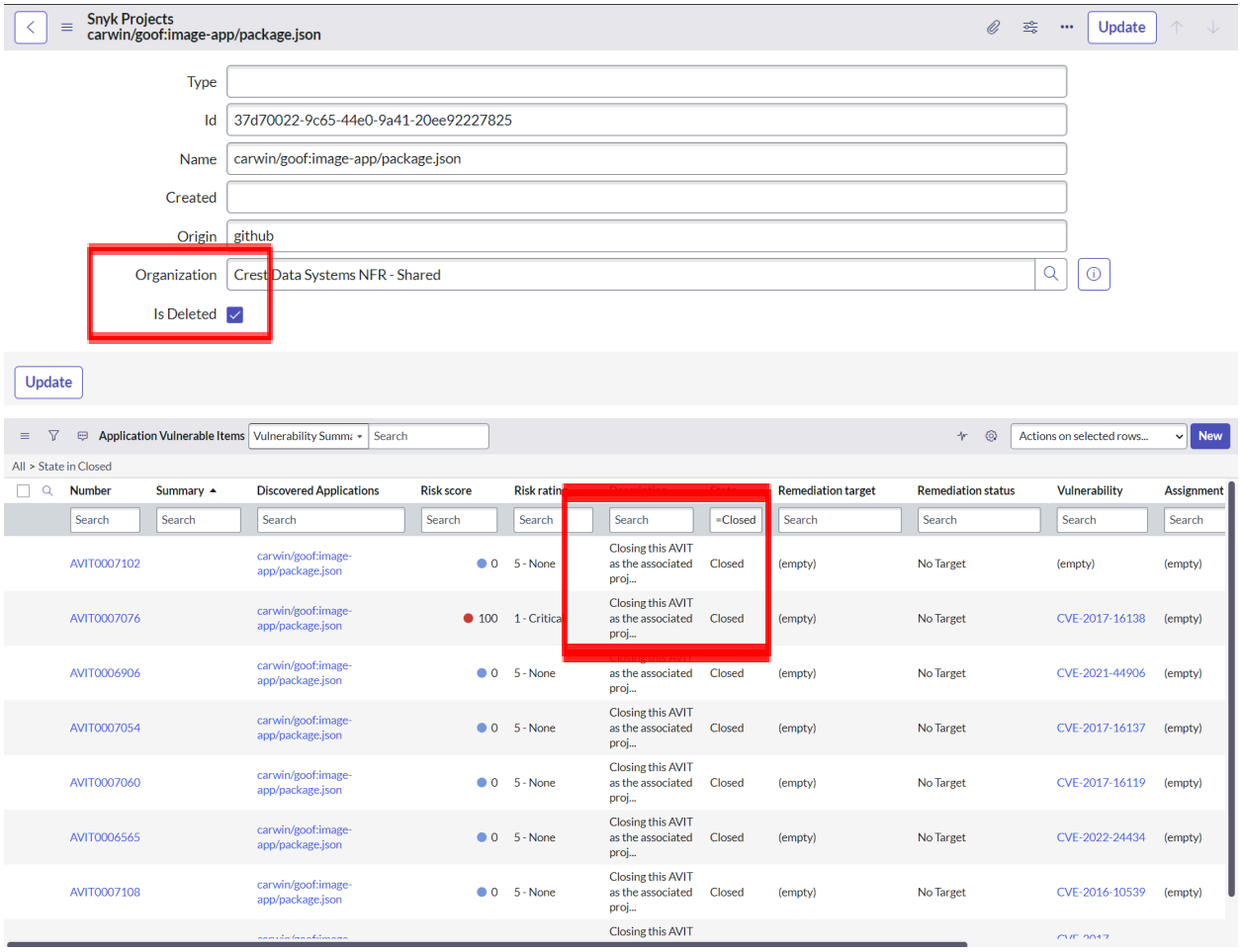


14. Packages will be visible in the list view of the "Package (sn_vul_app_package)" table.

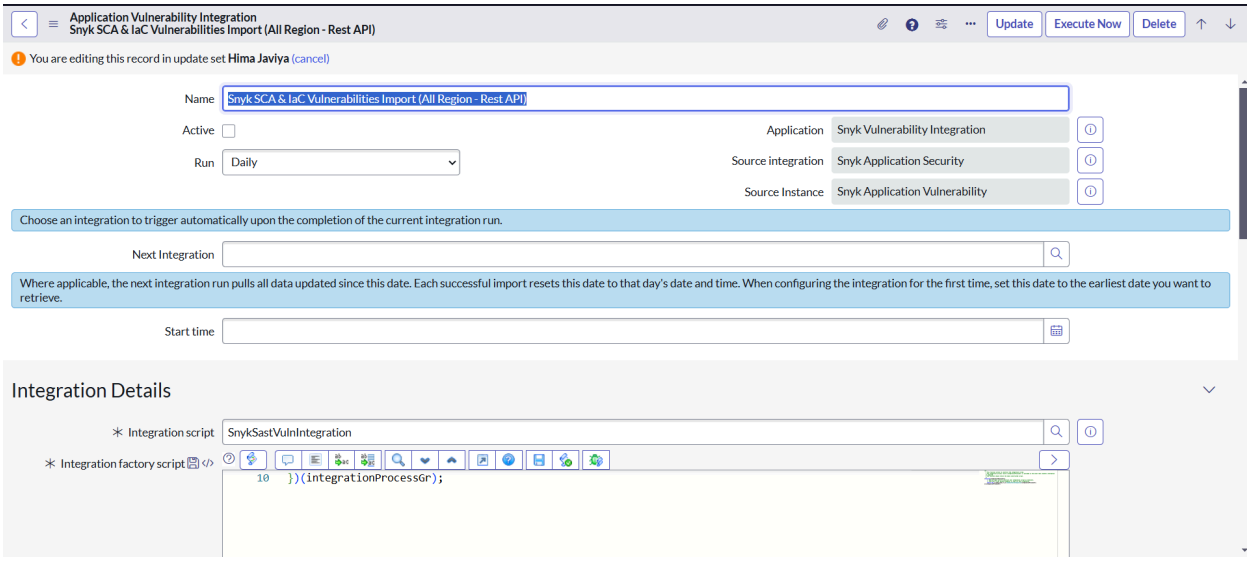
15. Users will have to provide the filter as "Source" "is" "Snyk" and then click on "Run" to view all of the packages that are fetched from Snyk.



16. If a project is deleted or deactivated after the AVIT is created, the AVIT state will be closed with a proper note in the Description.



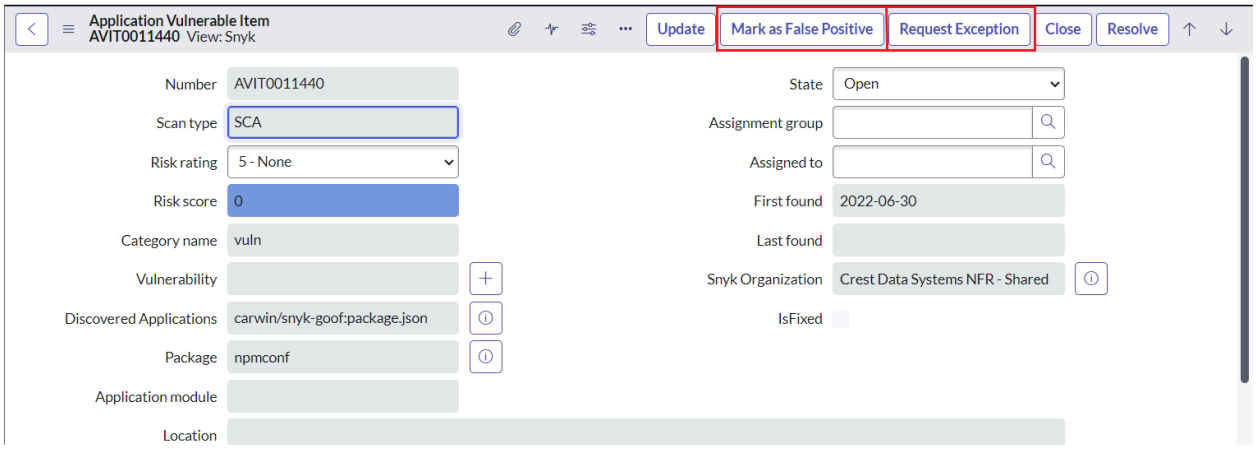
17. If the user marks an AVIT as "Mark as False Positive" or "Request Exception," the AVIT state will be set to "In Review." Once the request is approved, the "Additional

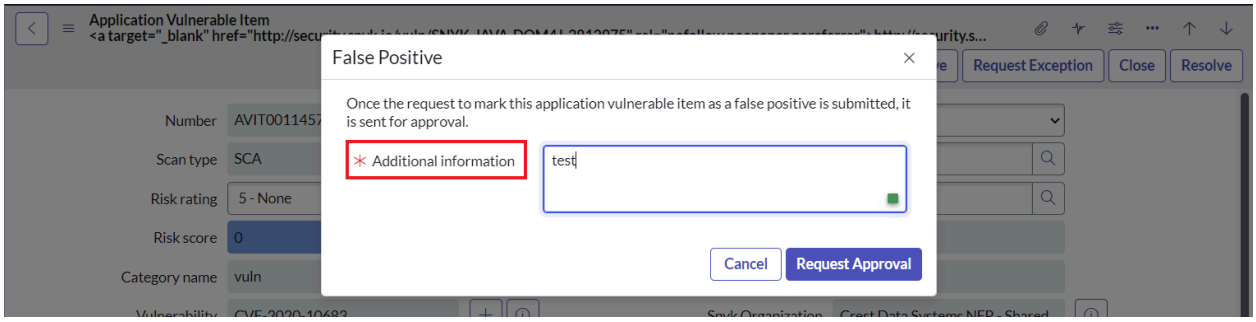


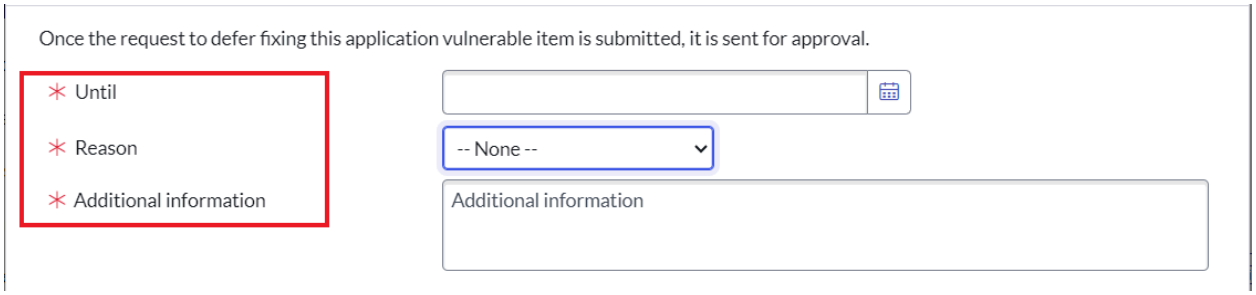
comment," "Until date," "Reason," and "Additional comment" in the request exception

added by the user will be added to the Snyk platform user interface. The AVIT state will be set to "Closed" after an approver approves the request.

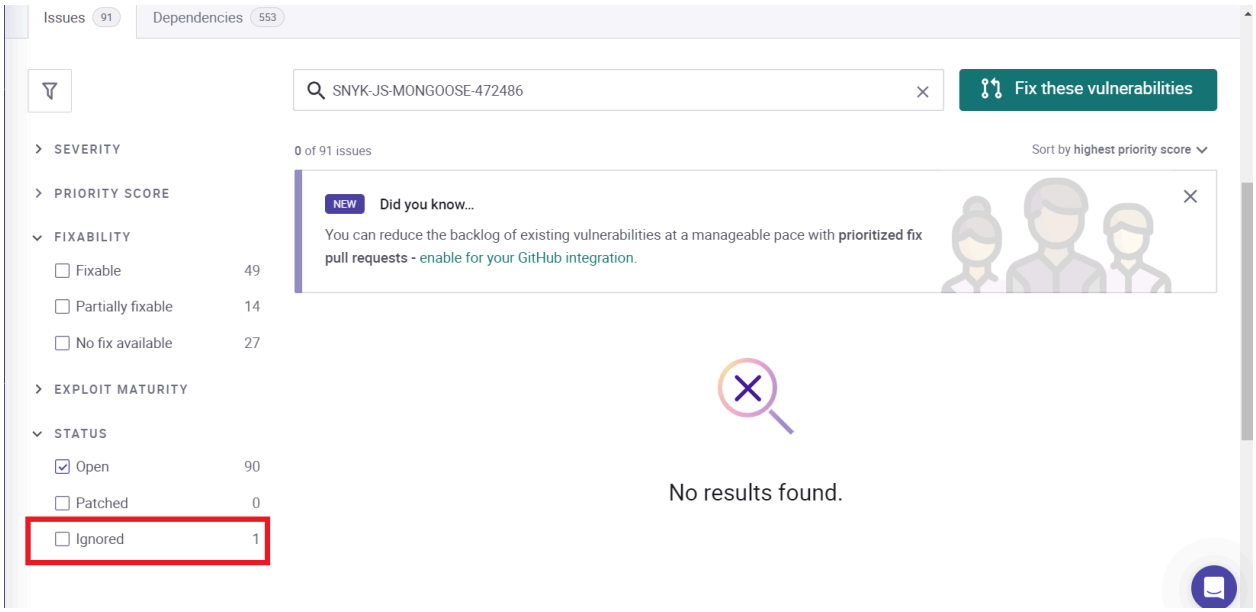
Note: The "Mark as False Positive" and "Request Exception" buttons will only be visible when the "Manage Exception in ServiceNow" & "Manage False Positive in ServiceNow" flag are set to "true" in the Vulnerability Filtering section.



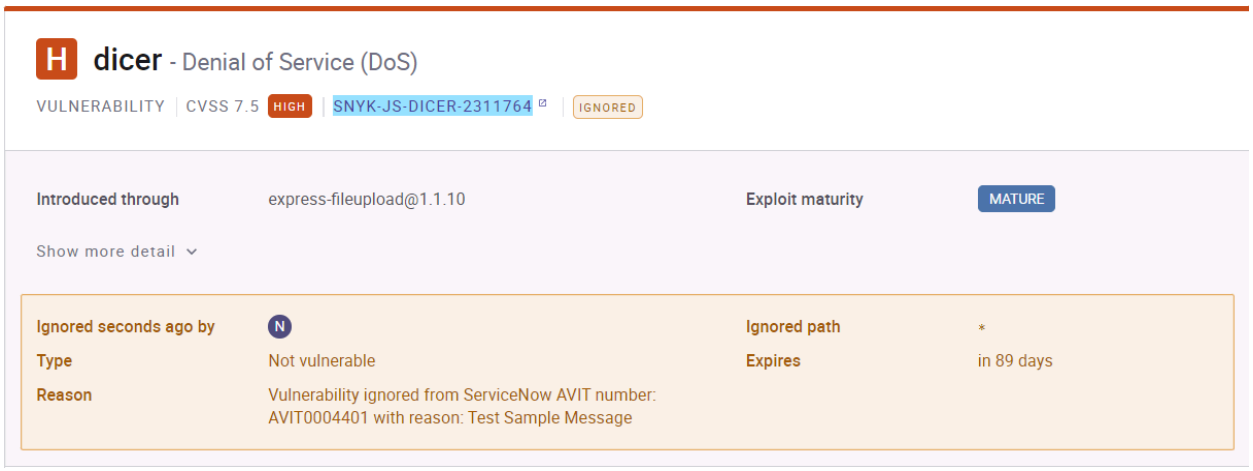




Once the AVIT is "Approved" and the state is changed, the user will be able to see the "Additional information" added to the issue on the Snyk platform. Users need to click on the "Source link" in the Findings of the AVIT, which will redirect to the Snyk platform on the Issues page. Then the user needs to add an "ignored" parameter in the filter.



Users will be able to see the issue with the comment. The comment will include the AVIT Number with the reason added from the ServiceNow side.



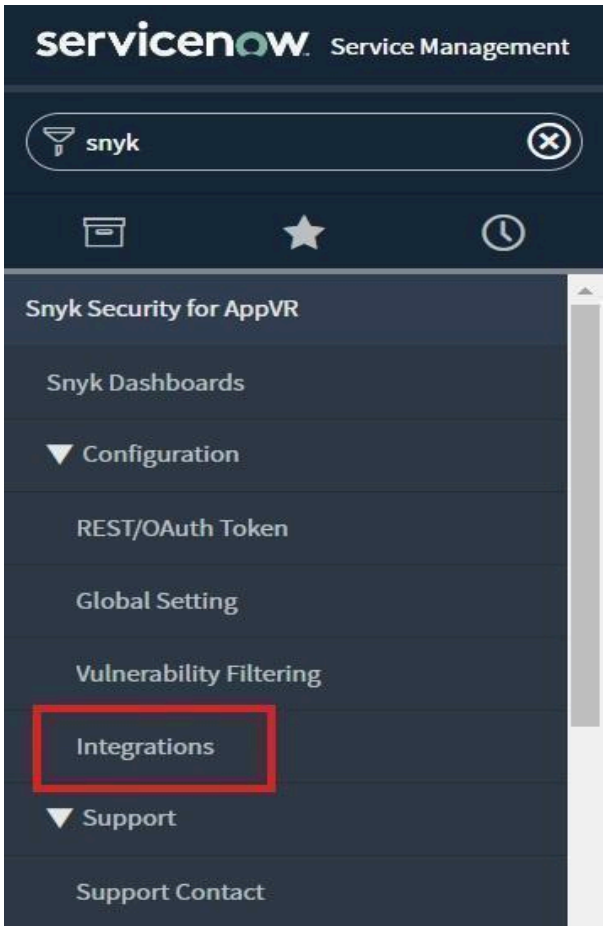
4.6. Fetch Issues from Snyk All Region SCA & IaC Vulnerability integration

"Snyk Security for AppVR" provides the functionality to fetch Issues from other regions (besides the US) and populates them as Vulnerability, Application Vulnerable Item, and Application Scan Summary in ServiceNow.

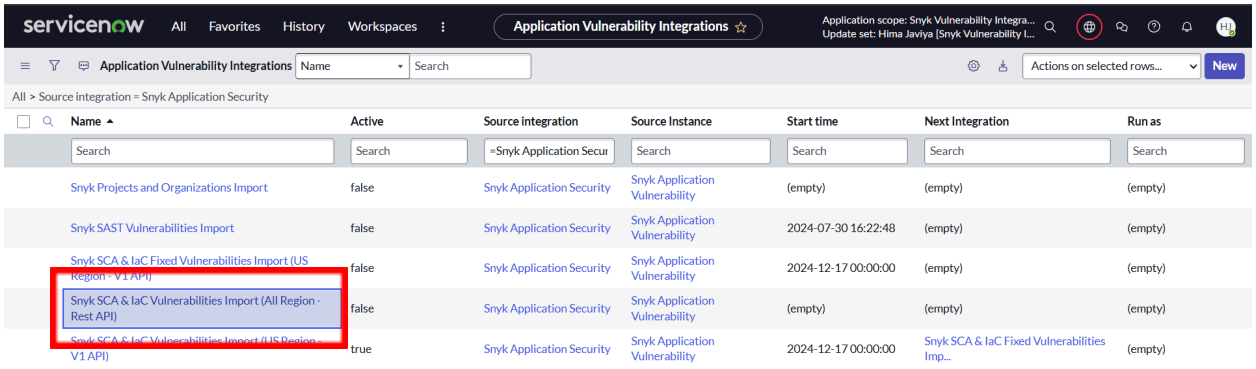
Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR" and select "Configuration."
3. Click on "Integrations."

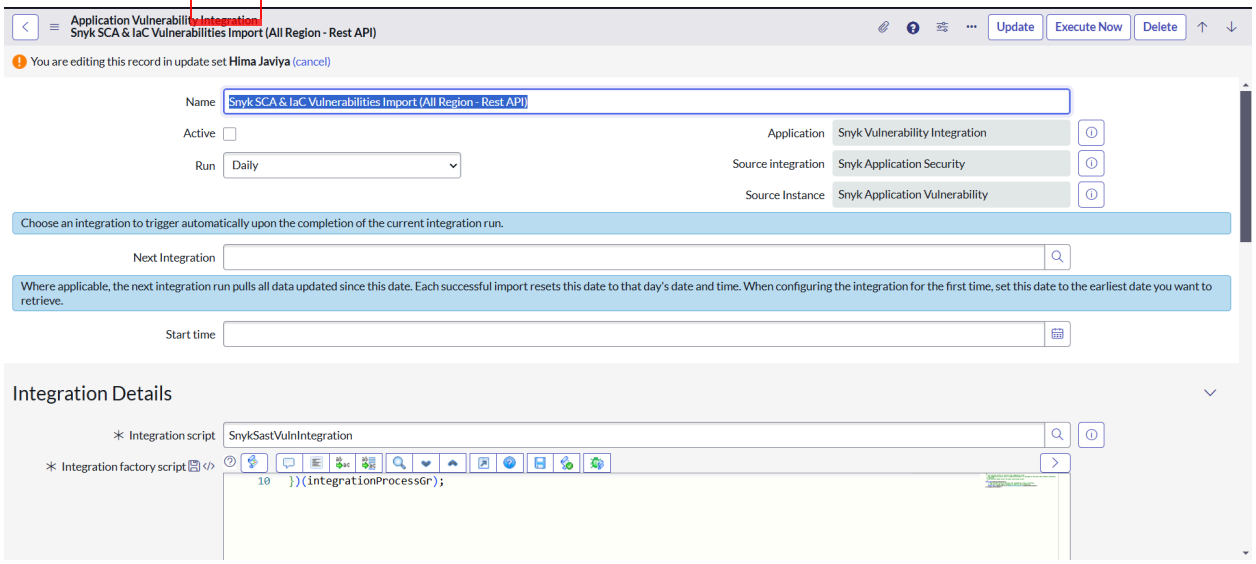


4. Click on the "Snyk SCA & IaC Vulnerability Import (All Region - Rest API)" integration.

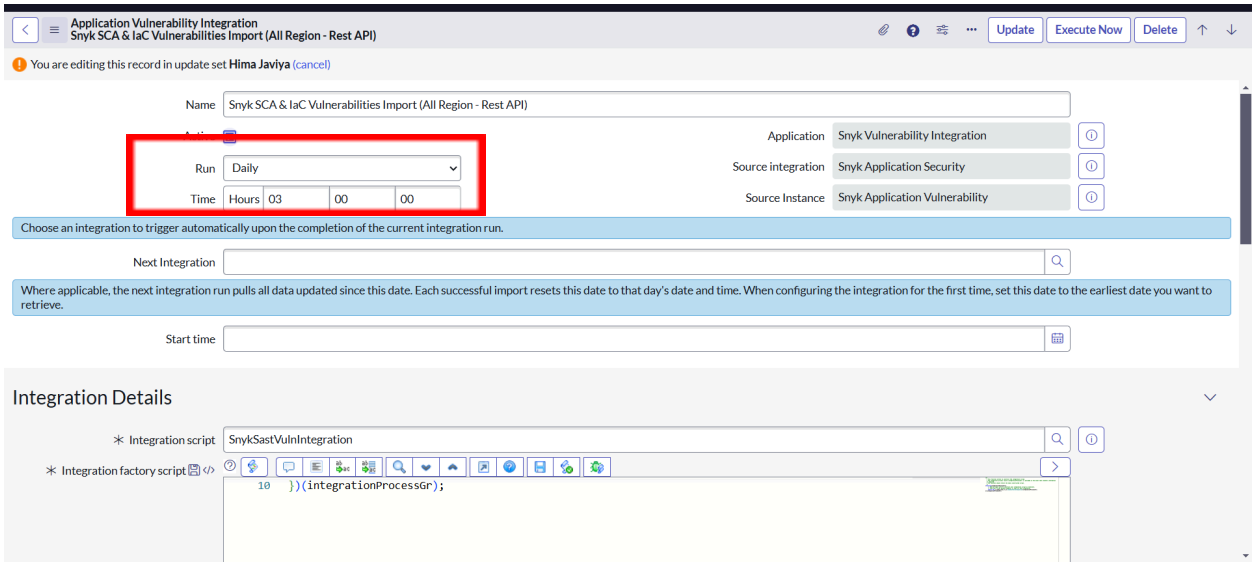


5. Activate the checkbox "Active." Click on the button "Update."

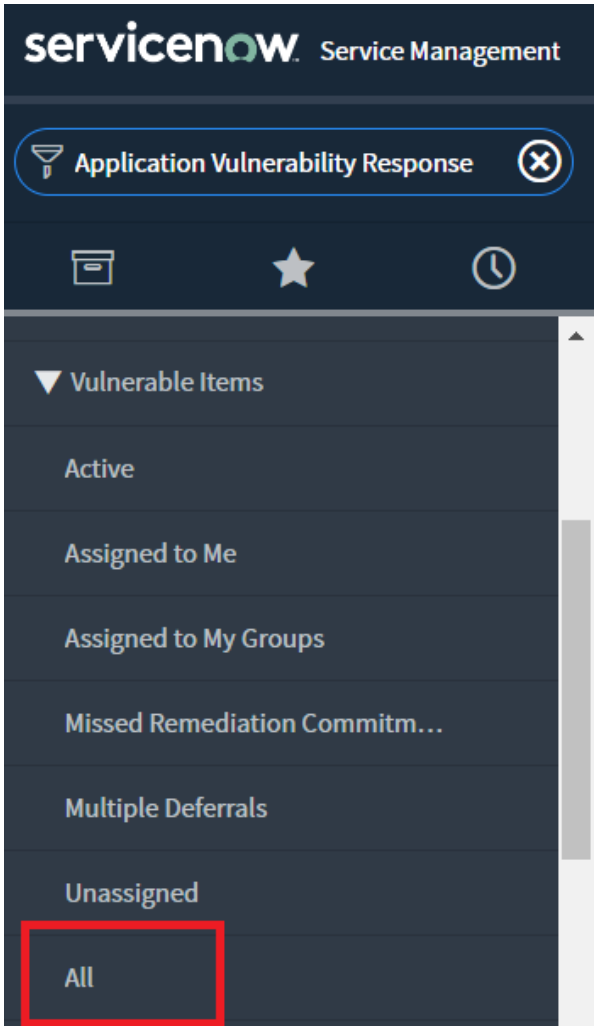
6. Open the Snyk Vulnerabilities Import (Only for EU and AU region) record. To fetch issues, click on the "Execute Now" button.



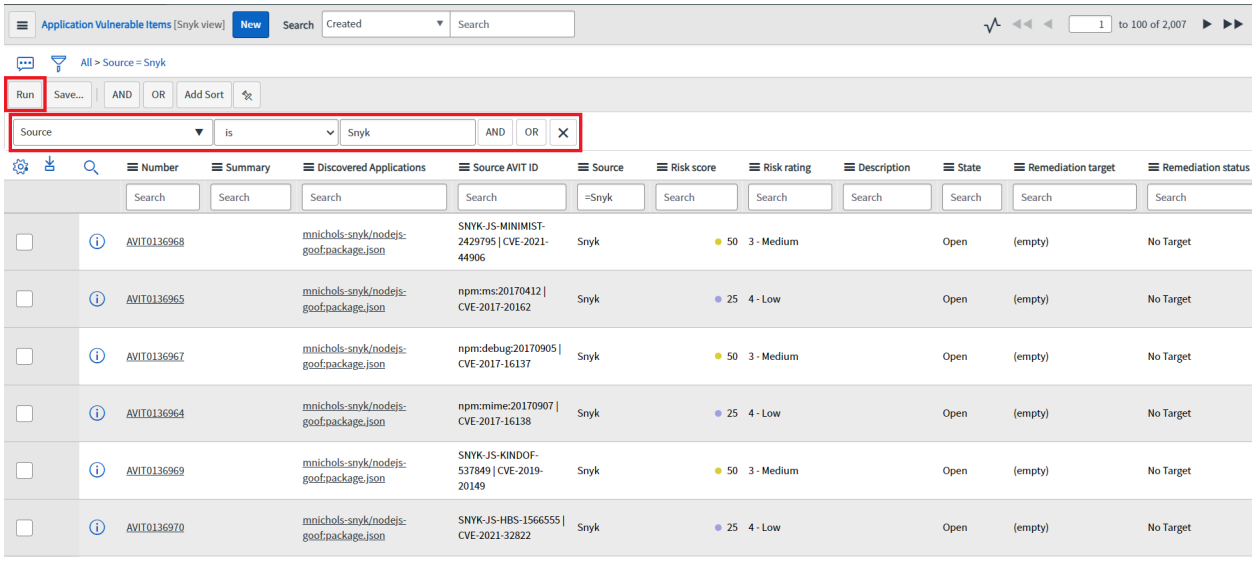
7. To fetch issues according to a scheduled time interval, select the relevant option from the Run dropdown, set the time, and click the "Update" button.



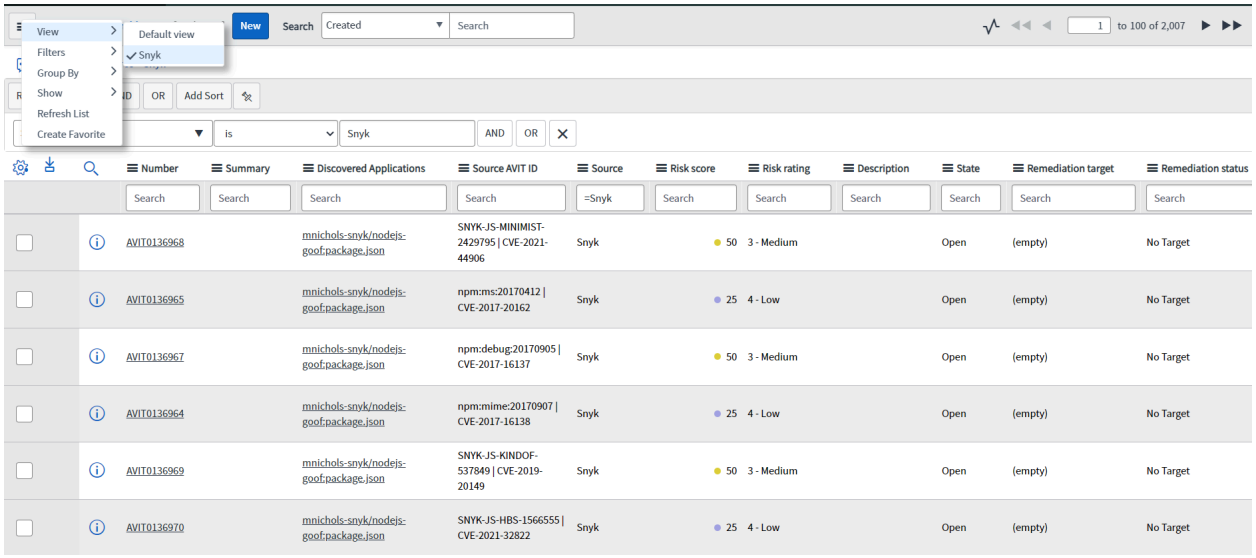
8. To view imported issues, navigate to "Application Vulnerability Response." Expand "Vulnerable Items," and under it select "All."



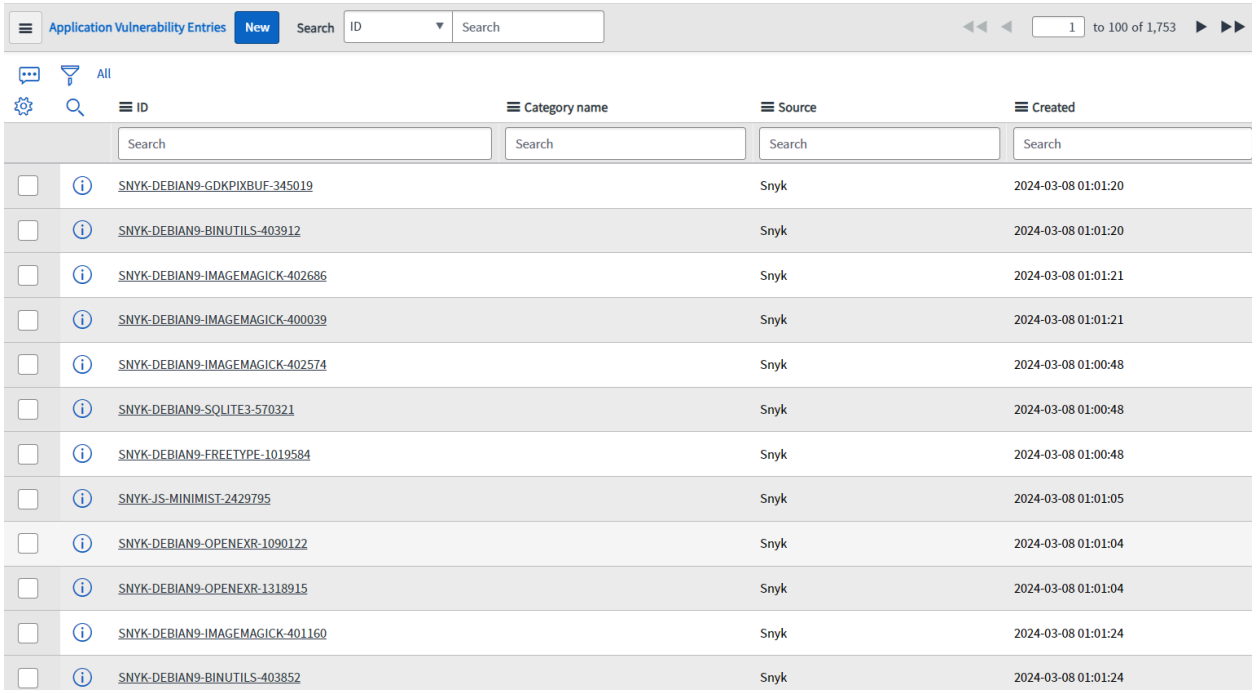
9. Users will have to provide the filter, as "Source" is "Snyk," and then click on "Run" to view all the issues fetched from Snyk.



10. Change the view to "Snyk" to view the "Snyk Priority Score" in the AVIT table.



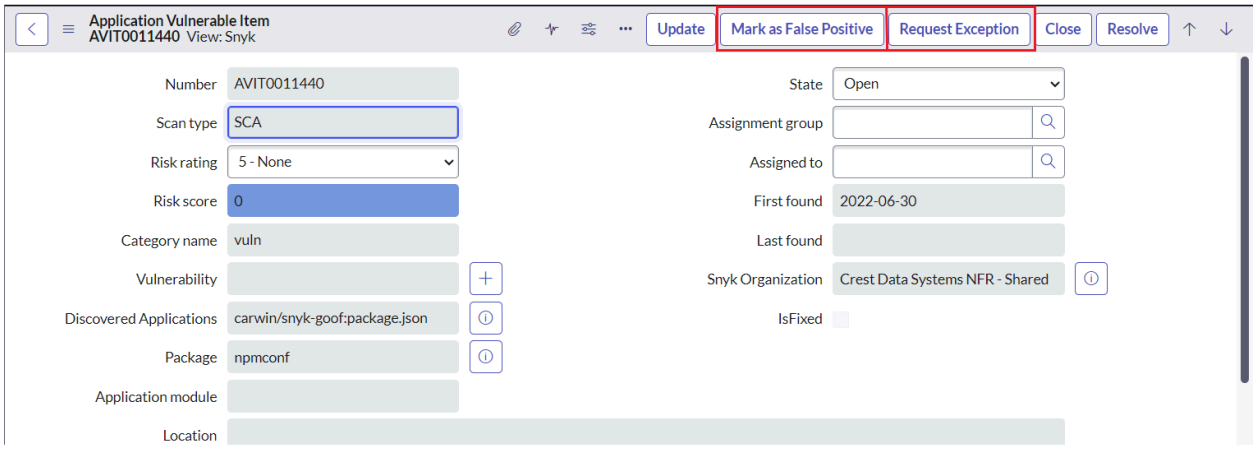
11. Third-party vulnerabilities will be visible in the list view of the "Application Vulnerability Entries (sn_vul_app_vul_entry)."
    Note: Third-party vulnerability will only be created when the Snyk issue does not contain CVEs in the identifiers.

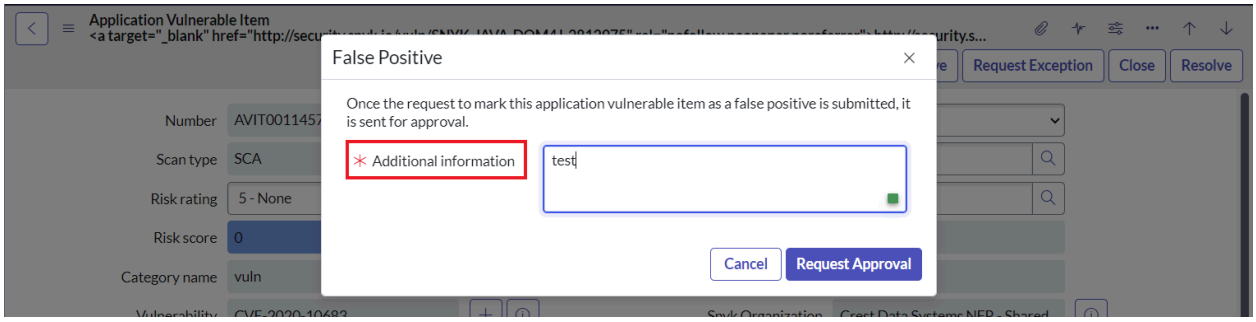


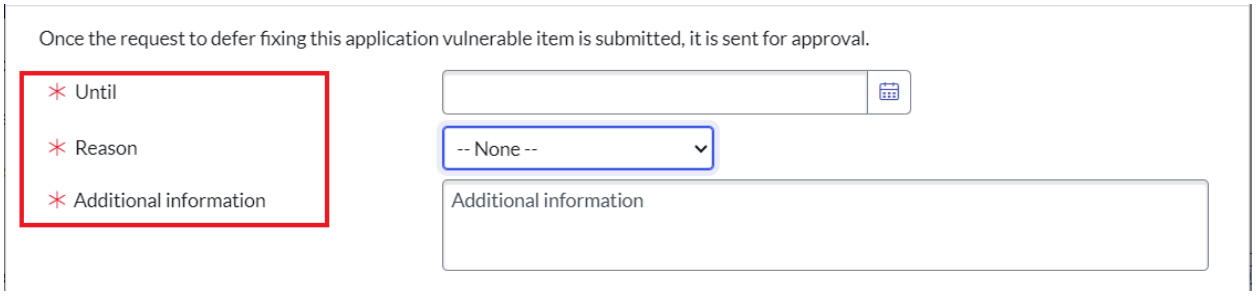
12. Packages will be visible in the list view of the "Package (sn_vul_app_package)" table.
13. Users will have to provide the filter as "Source" is "Snyk" and then click on "Run" to view all the packages fetched from Snyk.

14. If the user marks an AVIT as "Mark as False Positive" or "Request Exception," the AVIT state will be set to "In Review." Once the request is approved, the "Additional comment," "Until date," "Reason," and "Additional comment" in the request exception added by the user will be added to the Snyk platform user interface. The AVIT state will be set to "Closed" after the request is approved.

Note: The "Mark as False Positive" and "Request Exception" buttons will only be visible when the "Manage Exception in ServiceNow" & "Manage False Positive in ServiceNow" flags are set to "true" in the Vulnerability Filtering section. **AVITs created for IaC issues using the REST Integration do not support Mark as False Positive and Request Exception.**







Once the AVIT is "Approved" and the state is changed, the user can see the "Additional information" added to the issue on the Snyk platform. Users must click on the "Source link" in the AVIT's Findings, redirecting them to the Snyk platform on the Issues page. Then, the user needs to add an "ignored" parameter in the filter.

Note:

1) The Vulnerability Filters that work for this integration are Projects, Organizations, Ignored, and Status.
2) The fixed Snyk SCA & IaC Fixed Vulnerabilities Import will not work for this integration.
3) The default run time is 00:00 for this integration.

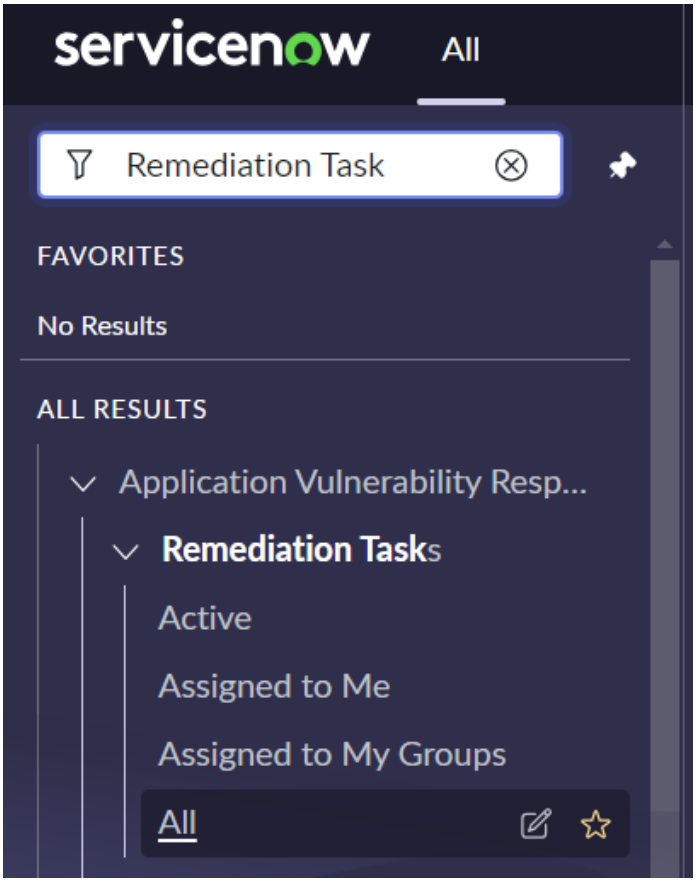
4.7. Bulk ignore of Application Vulnerable Items (AVITs) using Remediation tasks

This section describes how to use a Remediation task to ignore a group of Snyk issues from ServiceNow to Snyk.

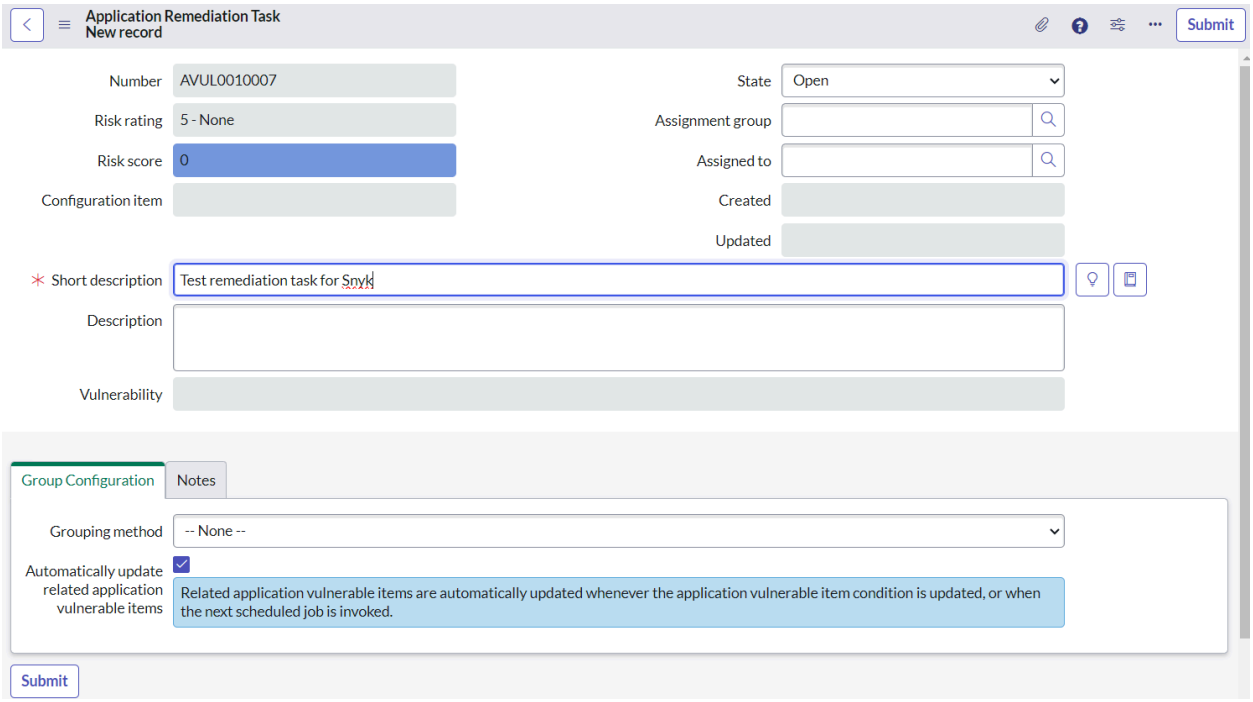
Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

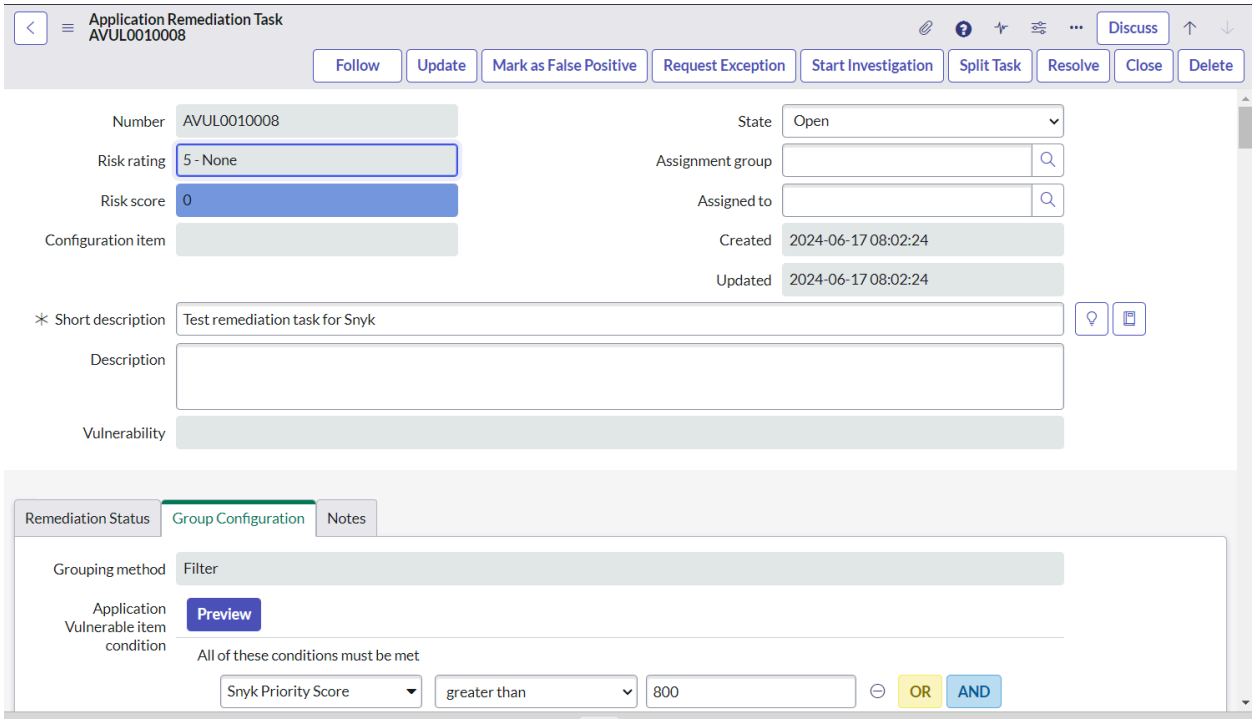
1. Login to the ServiceNow instance.
2. Navigate to Remediation Task under Application Vulnerability Response.



3. Click on All.
4. Click on the Create New button to create a new remediation task.



5. Fill in the mandatory fields. Check all field descriptions here
6. Choose the Grouping method based on your requirements. Click on the submit button to create the record.
7. Open the newly created Remediation Task.



8. To permanently ignore all the issues, select "Mark as False Positive." Otherwise, click on Request Exception with a specific period.
9. Once the button to run the action is clicked, the request is sent for approval to the approver user/group.
10. To approve the exception, an approver has to approve the request. Please review the link for more information - https://docs.servicenow.com/bundle/washingtondc-security-management/page/product/vulnerability-response/task/vr-ws-approve-requests.html

Note: IaC AVIT fetched from REST Integration does not support Bulk ignore issues.

4.8. Unignore issues from ServiceNow to Snyk

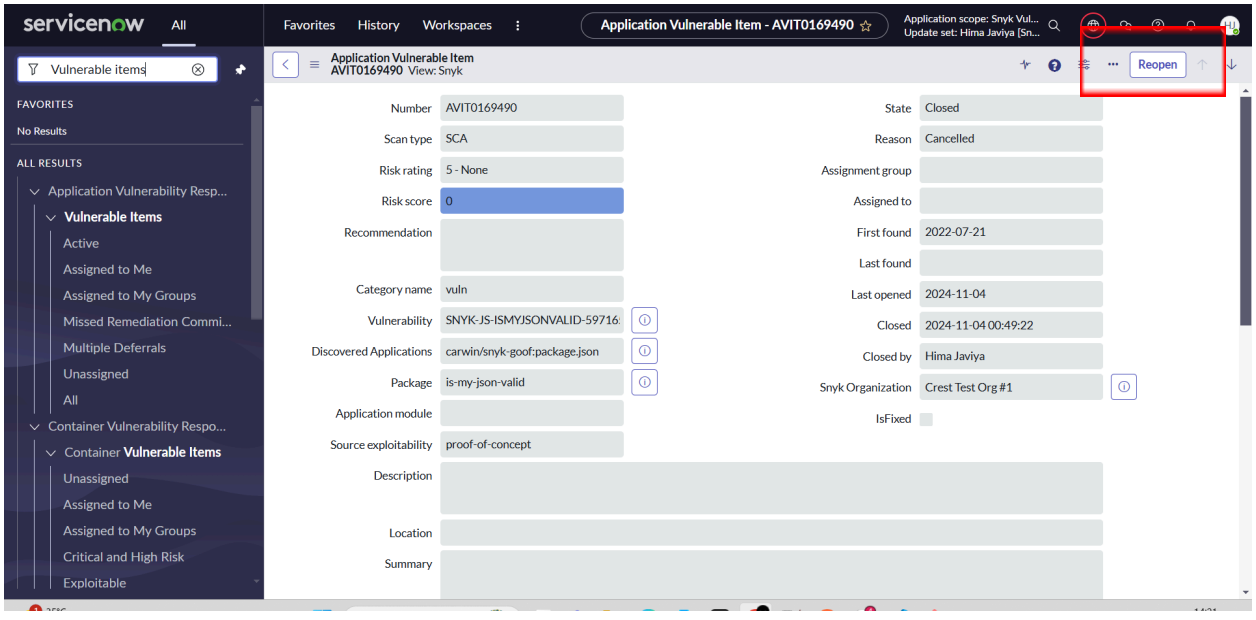
This section describes how to unignore a Snyk issue from ServiceNow to Snyk that has been previously ignored in ServiceNow.

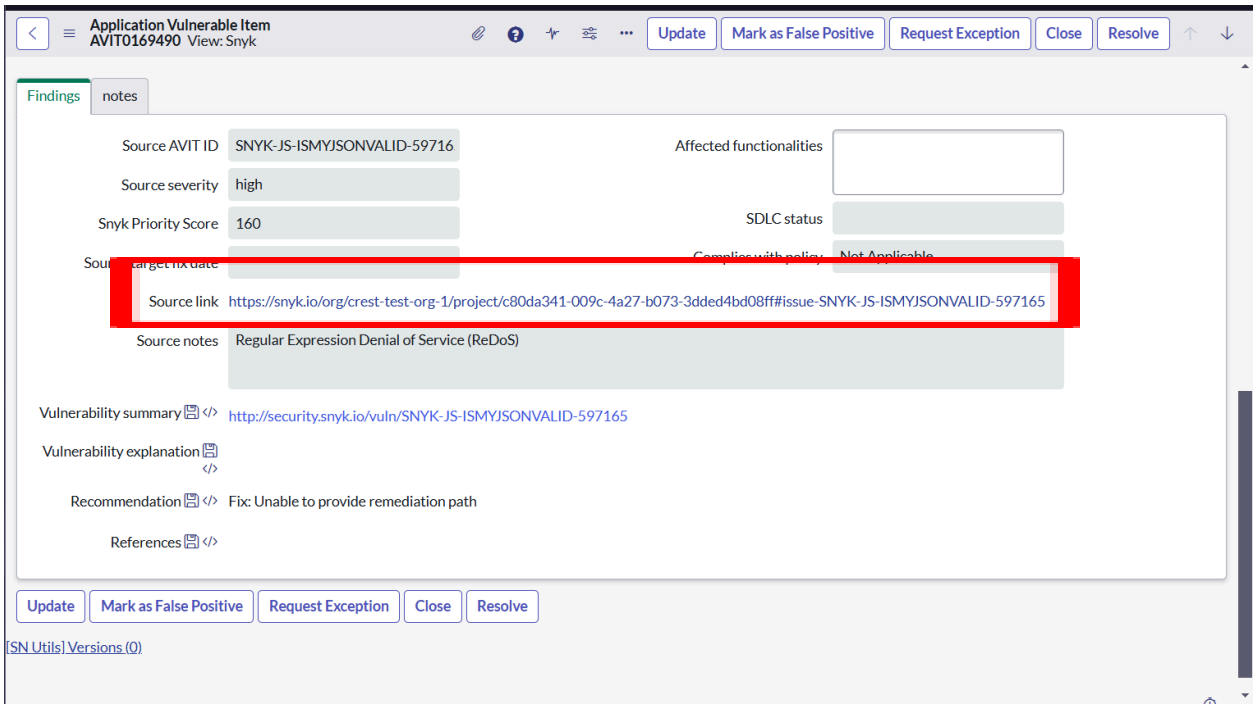
Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Navigate to Applications Vulnerability Response > Vulnerable Items > All.
2. Select the Closed AVIT you want to reopen in ServiceNow.

3. Click on Reopen, and the issue will be unignored in Snyk..





4. Click on the Source link to verify the ignored has been removed in Snyk.

Note: AVITs for Iac Issues fetched using the REST Integration do not support Unignoring issues.

4.9. Automatically Ignore and Unignore AVITs using Exception Rules

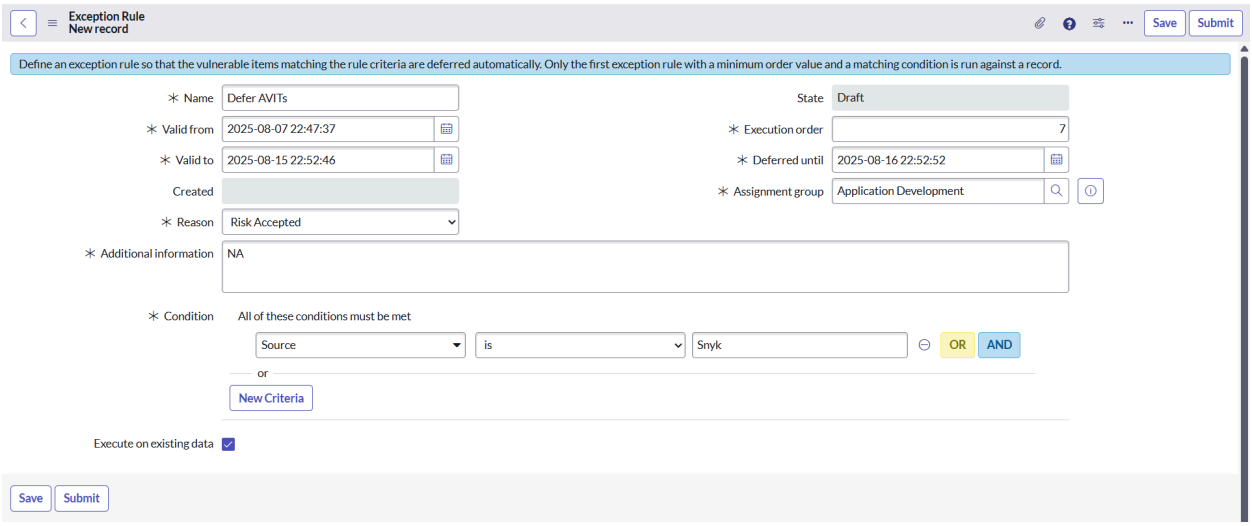
Exception rules let you automate the deferral of vulnerable items that cannot be remediated immediately. By defining specific conditions – such as affected vulnerabilities, configuration items (CIs), or VIs, these rules automatically defer matching items for a defined period. More details about exception rules can be found here.

This section describes how to automatically ignore & unignore a list of Snyk issues (AVITs) from ServiceNow to Snyk using Exception rules.

Role Required : sn_vul.app_manage_auto_exception_rule

Procedure :

1. Navigate to All > Application Vulnerability Response > Administration > Exception Rules.
2. Create a new Exception rule specify the filter conditions submit & Approve it.



3. Once the exception rule is approved, a remediation task is created in a deferred state. Starting from the **"Valid from"** to **"Valid to"** date, the exception rule runs on all the AVITs that are
    a. newly created
    b. moved from the Closed to the Open state.
    c. If “execute on existing data” is enabled then a scheduled job runs once on the existing data on the "Valid from" date.

    After the **“Deferred until”** date the exception rule expires and all the AVITs are moved to open state again.
4. When an AVIT is moved to the **Deferred** state by an exception rule, it is also automatically **marked as "ignored"** in the Snyk platform, with the **expiration date** set to the **"Deferred Until"** date defined in the exception rule.
5. When an AVIT is moved to **open** state from **deferred** due to expiration of the exception rule, the same ignore is unignored from the Issue in Snyk platform.

Note: After version 26.0.11 of VR, exception rules no longer create remediation tasks. Instead, VITs are deferred directly without being associated with a remediation task.

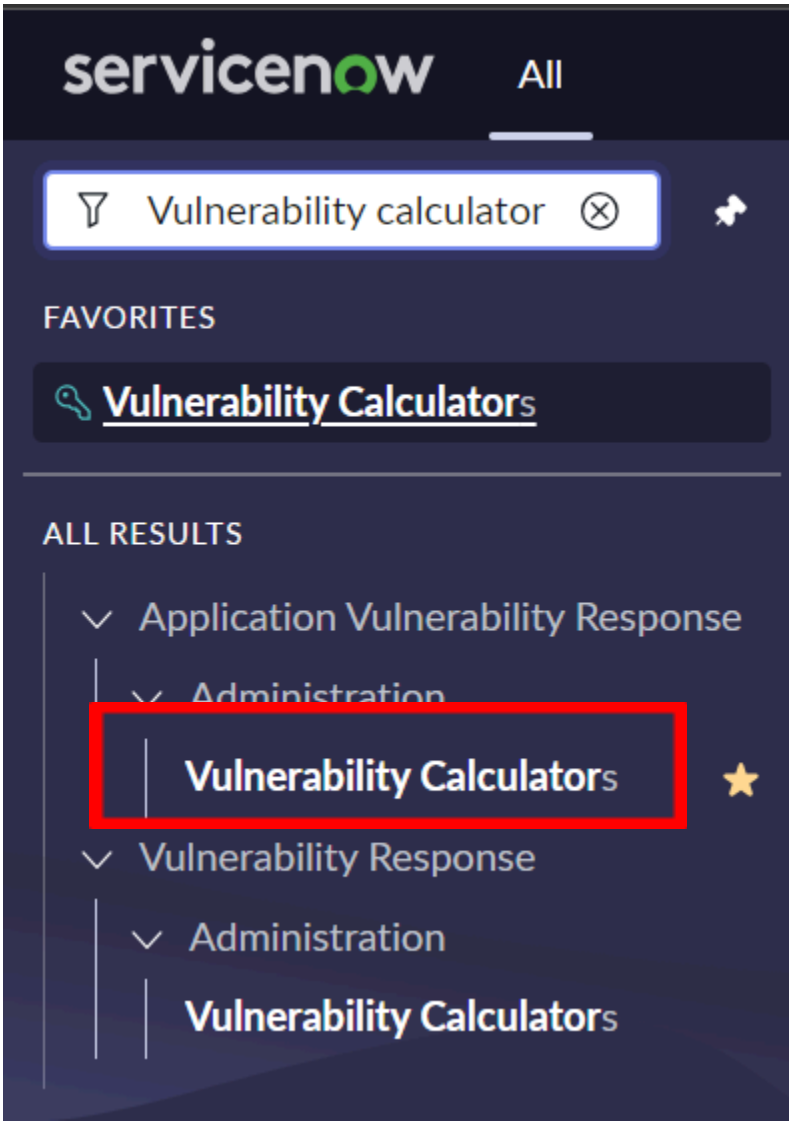
4.10. Snyk Risk Score Calculator

The Snyk risk score calculator calculates the risk rating and risk score based on the Snyk priority score. It can be used to define a risk score for an AVIT when automatically generating AVITs from vulnerabilities identified by Snyk.

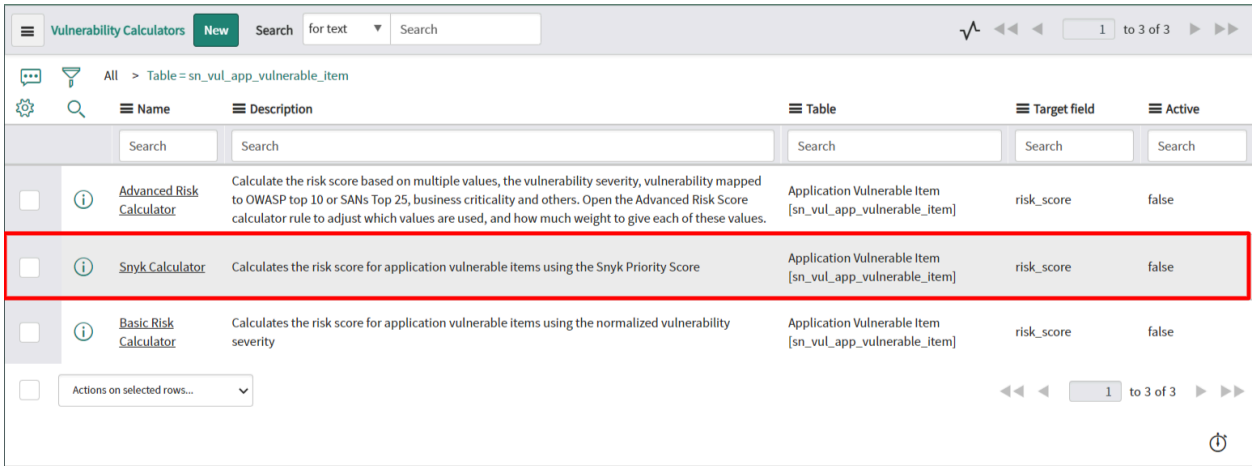
Role Required: sn_vul.app_manage_risk_score_configuration

Procedure:

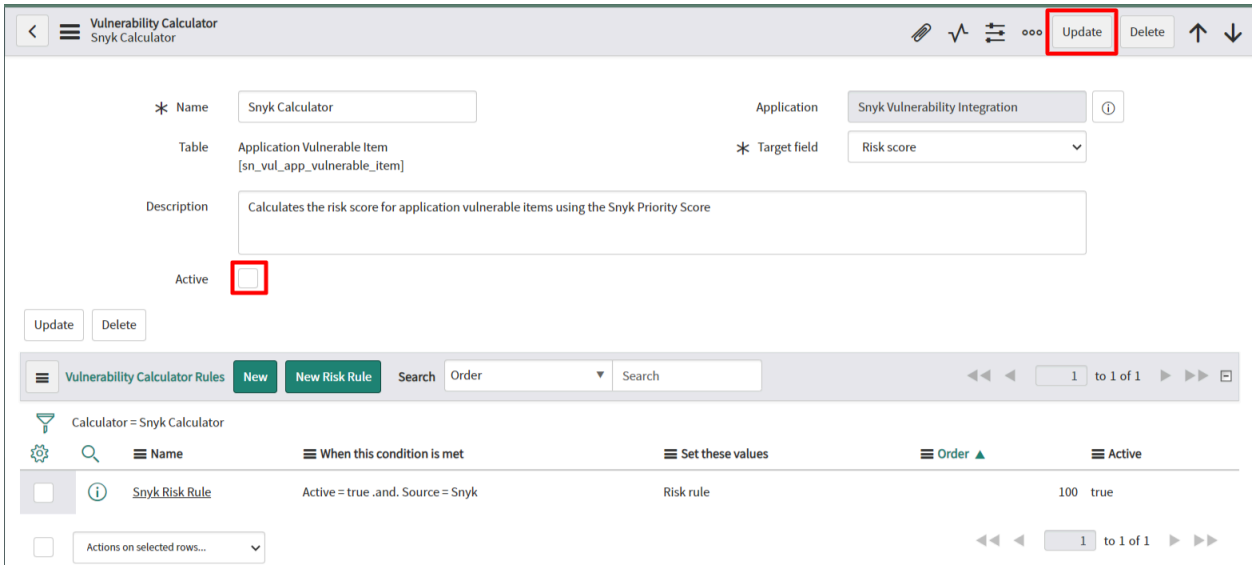
1. Login to the ServiceNow instance.
2. Navigate to the "Application Vulnerability Response"
3. Click "Administrator" and select "Vulnerability Calculator" from the dropdown menu.



4. Select "Snyk Calculator."



5. Activate the Snyk calculator by clicking the active checkbox and then update the record.



6. **Note: Activating the Snyk risk score calculator will only calculate the risk score of AVITs whose source is Snyk. If the user wants to calculate the risk score of AVITs for other sources, they can create a new risk rule for them in the Snyk calculator or create a new calculator.**

7. If you want to create your own calculator or modify the existing calculator, then click this.

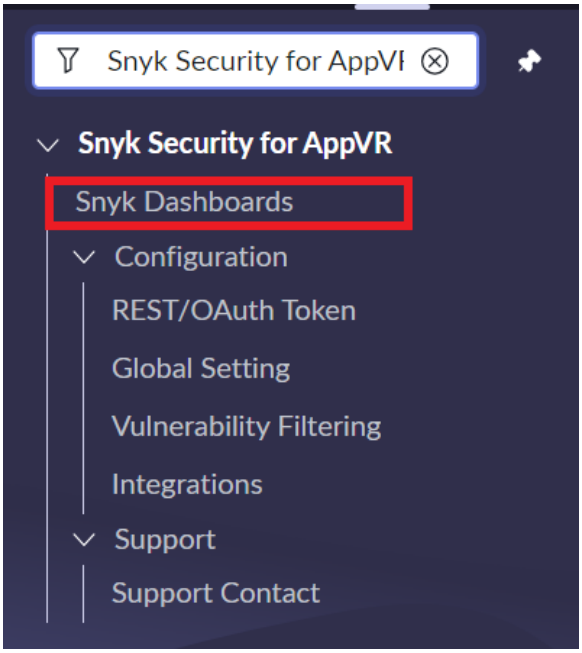
4.11. Snyk Dashboard

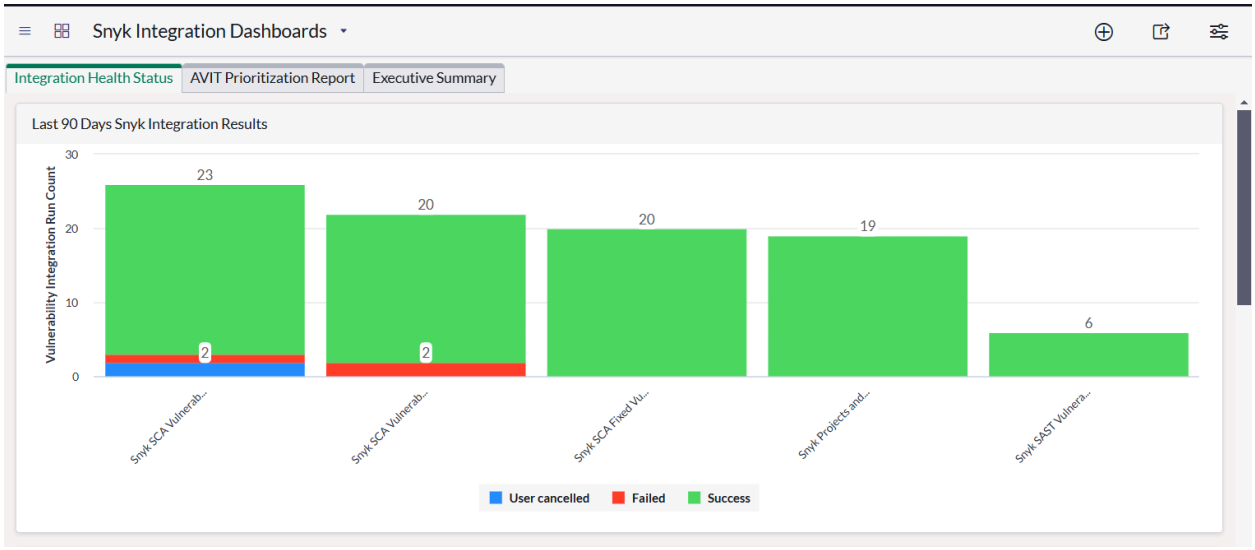
"Snyk Security for AppVR" provides the functionality to view the dashboard and provide an overview of the data.

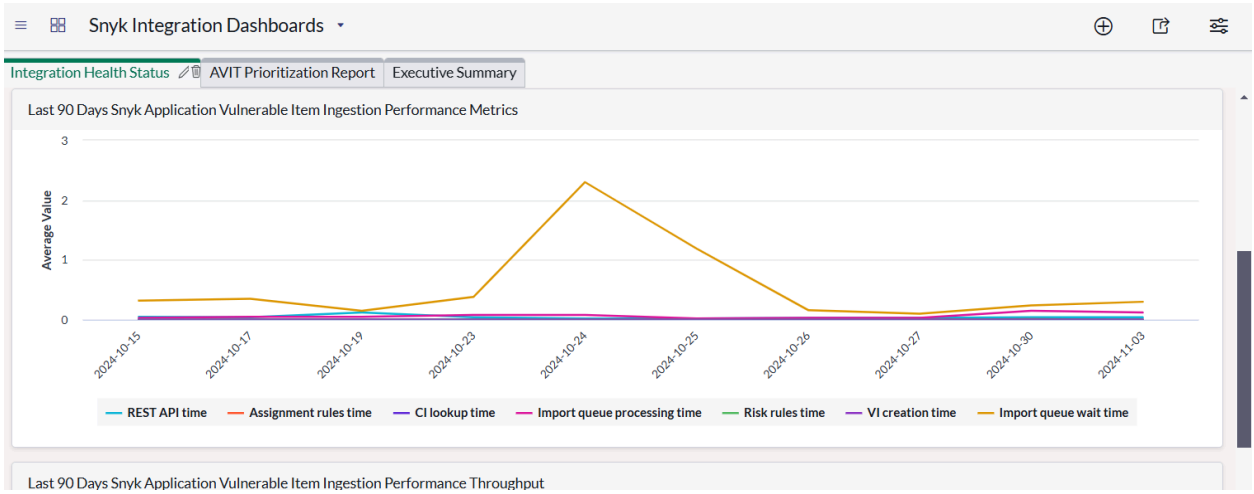
Role Required: x_snyk2_snyk_vr_in.configure_integration, sn_vul.configure_integrations, sn_vul.app_read_assigned

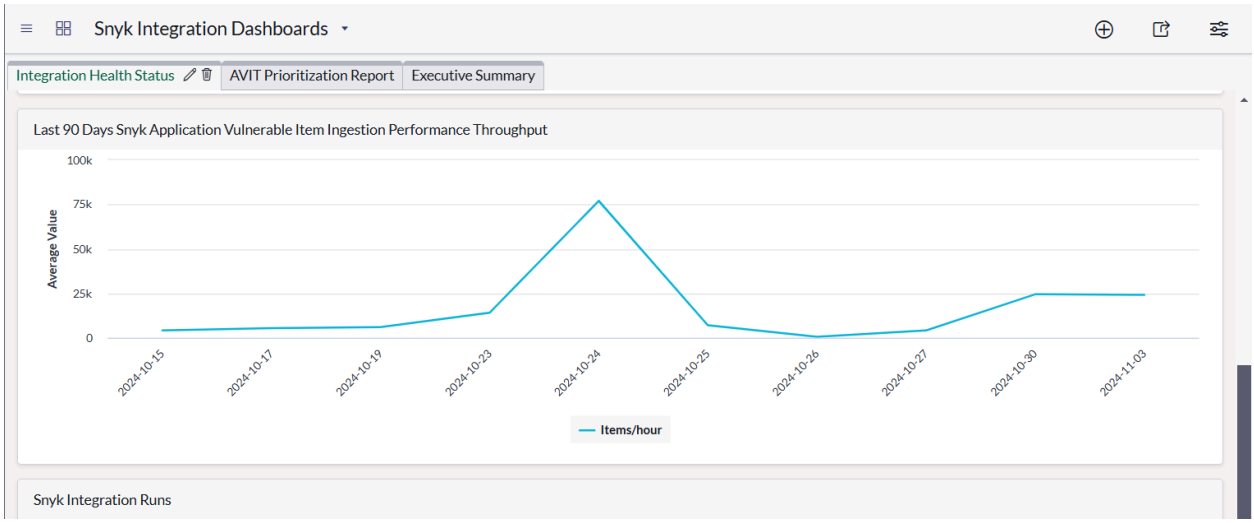
Procedure:

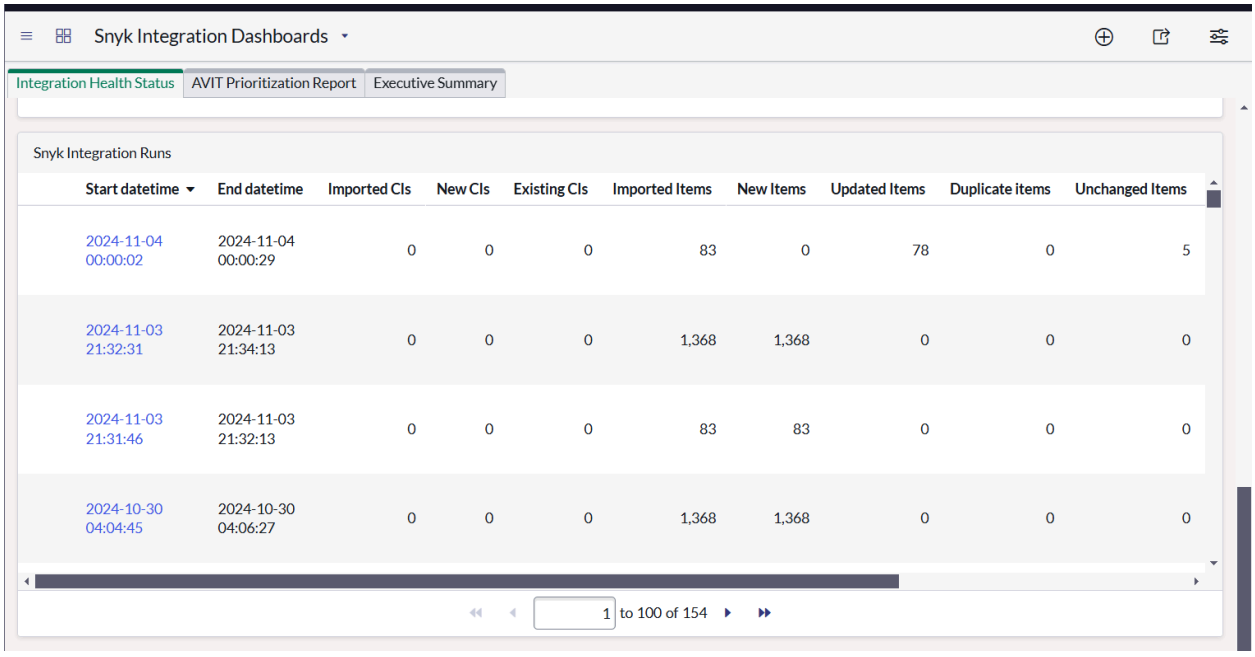
1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR."
3. Click on "Snyk Security for AppVR," and under it select "Snyk Dashboards."

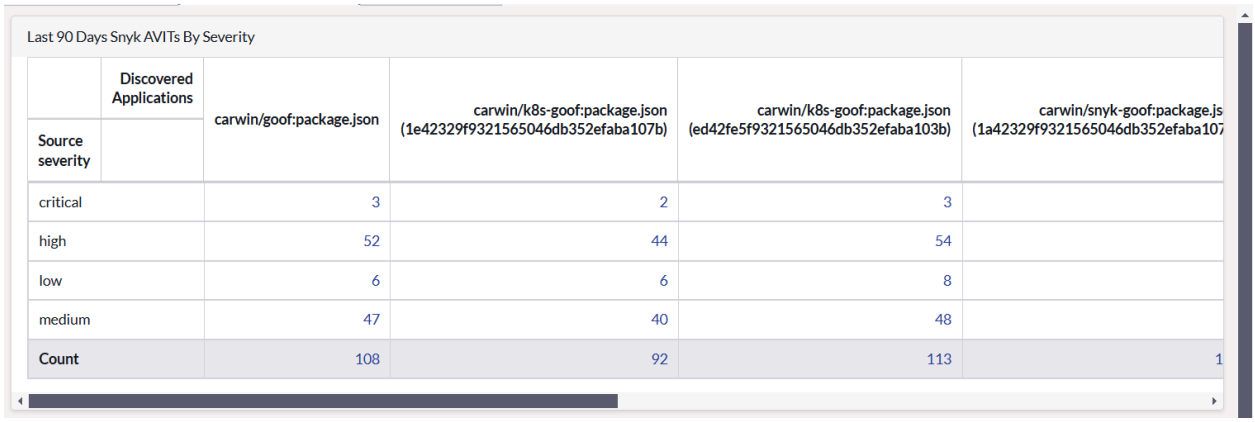





Snyk Integration Dashboards
Integration Health Status
AVIT Prioritization Report
Executive Summary
Last 90 Days Snyk Application Vulnerable Item Ingestion Performance Metrics
Average Value
3
2
1
0
2024-10-15
2024-10-17
2024-10-19
2024-10-23
2024-10-24
2024-10-25
2024-10-26
2024-10-27
2024-10-30
2024-11-03
REST API time
Assignment rules time
CI lookup time
Import queue processing time
Risk rules time
VI creation time
Import queue wait time
Last 90 Days Snyk Application Vulnerable Item Ingestion Performance Throughput

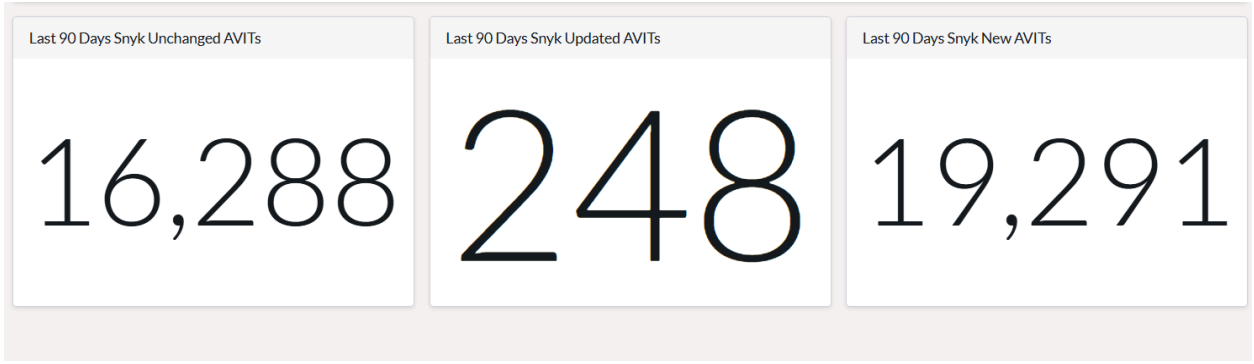

Snyk Integration Dashboards
Integration Health Status
AVIT Prioritization Report
Executive Summary
Last 90 Days Snyk Application Vulnerable Item Ingestion Performance Throughput
Average Value
100k
75k
50k
25k
0
2024-10-15
2024-10-17
2024-10-19
2024-10-23
2024-10-24
2024-10-25
2024-10-26
2024-10-27
2024-10-30
2024-11-03
Items/hour
Snyk Integration Runs


Snyk Integration Dashboards
Integration Health Status
AVIT Prioritization Report
Executive Summary
Snyk Integration Runs
Start datetime
End datetime
Imported CIs
New CIs
Existing CIs
Imported Items
New Items
Updated Items
Duplicate items
Unchanged Items
2024-11-04 00:00:02
2024-11-04 00:00:29
0 0 0 83 0 78 0 5
2024-11-03 21:32:31
2024-11-03 21:34:13
0 0 0 1,368 1,368 0 0 0
2024-11-03 21:31:46
2024-11-03 21:32:13
0 0 0 83 83 0 0 0
2024-10-30 04:04:45
2024-10-30 04:06:27
0 0 0 1,368 1,368 0 0 0
1 to 100 of 154



Last 90 Days Snyk AVITs By Severity

Source severity	Discovered Applications	carwin/goof:package.json	carwin/k8s-goof:package.json (1e42329f9321565046db352efaba107b)	carwin/k8s-goof:package.json (ed42fe5f9321565046db352efaba103b)	carwin/snyk-goof:package.js (1a42329f9321565046db352efaba107
critical		3	2	3	
high		52	44	54	
low		6	6	8	
medium		47	40	48	
Count		108	92	113	1



Last 90 Days Snyk Unchanged AVITs

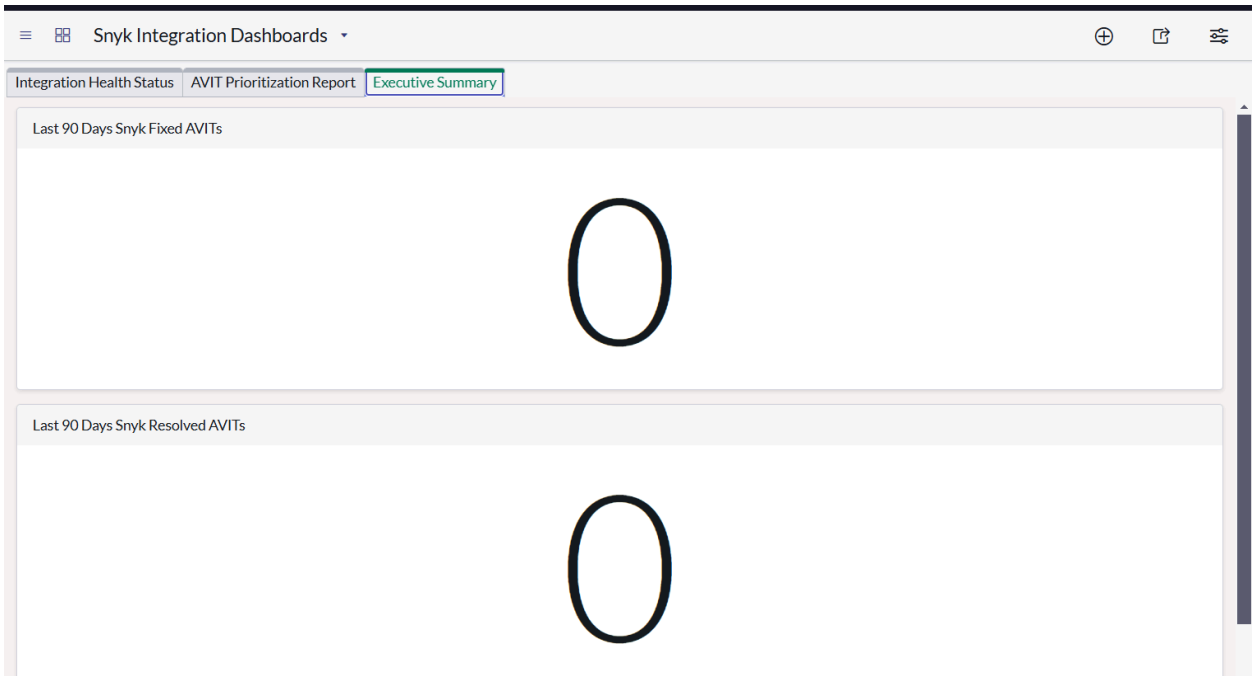
16,288

Last 90 Days Snyk Updated AVITs

248

Last 90 Days Snyk New AVITs

19,291



Snyk Integration Dashboards

Integration Health Status | AVIT Prioritization Report | Executive Summary

Last 90 Days Snyk Fixed AVITs

0

Last 90 Days Snyk Resolved AVITs

0

4.12. System properties (optional)

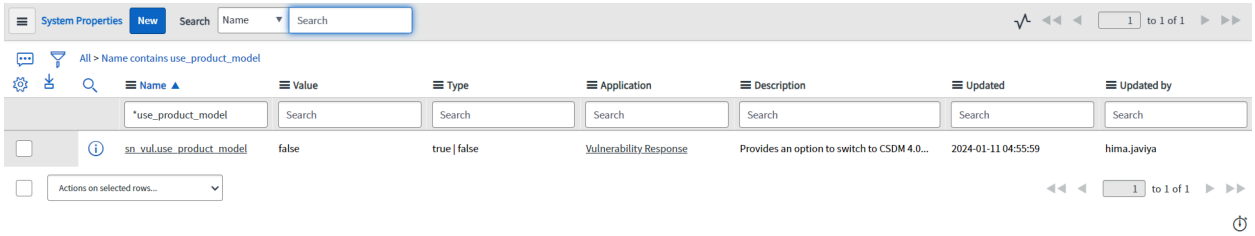
Role required: System Administrator

Update the values in the system properties only if required. Changing values of system property can impact the integration. Below are the details of the system properties. Users can go to system properties by typing sys_properties.LIST and the filtering properties with app scope.

Properties	Use Case
x_snyk2_snyk_vr_in.pageSize	Page size for SCA & IaC Issues for V1 Integration
x_snyk2_snyk_vr_in.pageSizeProjects	Page size for Projects
x_snyk2_snyk_vr_in.request_timeout	When making a Snyk API request, this time will be utilized to wait for a response (in seconds).
x_snyk2_snyk_vr_in.retry	The API call will be retried this many times.
x_snyk2_snyk_vr_in.until_date	This will be implemented when updating the state from ServiceNow to Snyk. If the "AVIT Request Exception until date" exceeds 365 days, the issue will be ignored permanently. The default value is set to 365 days, but you can adjust it to a value below 365 days as needed.
x_snyk2_snyk_vr_in.waitTime	Wait time for subsequent API calls if a timeout error occurs in Snyk API (in milliseconds).

4.13. CI LookUp rule

- Below are the steps to follow if your ServiceNow instance stores Snyk Applications in the **"sn_vul_app_scanned_application"** table and you want to create or use existing CIs (Configuration Items) when creating Discovered Applications for Snyk applications.
- Make sure the system property (**sn_vul.use_product_model**) is false. For verification, follow the steps below.
    - Navigate to **sys_properties.LIST**
    - Search for **sn_vul.use_product_model**

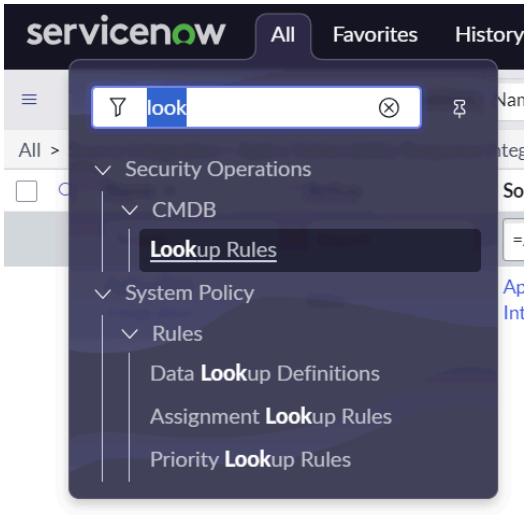


    - The value should be **false.** If not, change it to **false.**

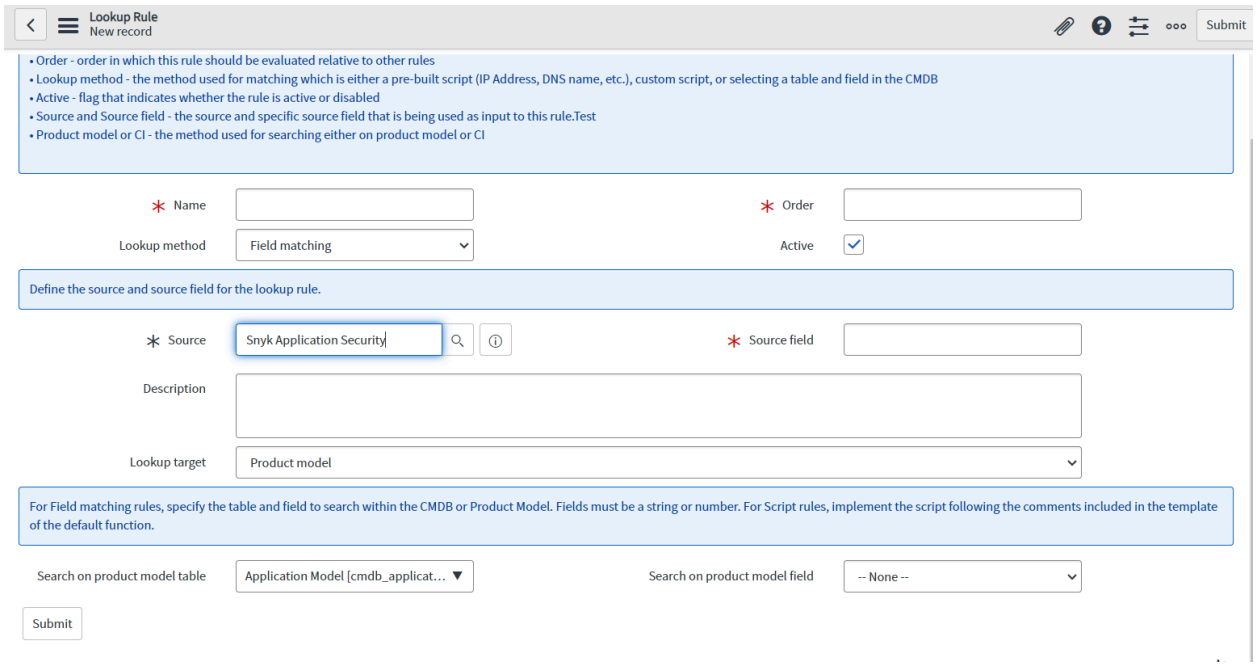
- If **the sn_vul.use_product_model** value is true, it will create a product model. If you choose that approach, you must create a Lookup rule with a lookup target Product Model.

Note: If your ServiceNow instance stores Snyk projects in a CMDB class other than the "**sn_vul_app_scanned_application**" table, then you need to create your own look-up rule but ensure you keep the source field as **source_app_id**. (**Note:** If you're using tags to match the record, then it will consider the tag value of the tag mentioned in the global settings module of the integration; otherwise, it will consider the project ID.) Follow the steps below to create the Lookup rule.

- Navigate to **Security Operations -> CMDB -> Lookup Rules.**



- Click on the New button to create a new Lookup rule.



- Give a Unique **Name**—for example, "Snyk Product Rule."

- Select "Field matching" in the **Lookup Method**. Use a custom script if the table is not present in the list.
- Select **Source** as Snyk Application Security.
- Select **Lookup target** as Product Model or Configuration item based on requirement.
- Select the Table name where your ServiceNow stored application data is **Search on the product table.**
- In the **Source field,** give the product table a unique name that should map to the application field name. (Application fields: app_name, source_app_id)
- Click on the **Update** Button.
- Similarly, users can create CI lookups for other CMDB tables if needed.
- Make sure your CMDB matching field has the exact same value as the Snyk project tags value/project ID to map correct CIs.
- **Note:** Any customization to the existing lookup rule or new lookup rule that is created will never override in future upgrades, as ServiceNow doesn't override customer updates by default.
- Refer to the link below for more info about creating CI Look-up rule: https://docs.servicenow.com/bundle/washingtondc-security-management/page/product/security-operations-common/task/create-ci-identifier-rules.html.
- From **v3.1.0 onwards**, the `sourcepayload` will include **full project details from the API**, enabling more advanced and specific **CI lookup rule matching**.

  The payload contains comprehensive project metadata, including:

  - Project ID, name, and type
  - Latest issue and dependency counts
  - Target file and Git reference
  - Origin and status
  - Organization and target relationships (including URLs)
  - Importer info
  - Project attributes (e.g., lifecycle, environment, tags)

Payload Example:


```
{
 "type": "project",
 "id": "50f158ef-6a8c-4c51-830c-baf16ed5d5a8",
 "meta": {
  "latest_issue_counts": {
   "updated_at": "2025-06-01T19:05:42.202Z",
```

```
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0
   },
   "latest_dependency_total": {
    "updated_at": "2025-06-01T19:05:42.202Z",
    "total": 0
   }
  },
  "attributes": {
   "name": "mnichols-snyk/strapi:package.json",
   "type": "yarn",
   "target_file": "package.json",
   "target_reference": "develop",
   "origin": "github",
   "created": "2024-11-20T16:06:20.419Z",
   "status": "active",
   "business_criticality": [],
   "environment": [],
   "lifecycle": [],
   "tags": [],
   "read_only": false,
   "settings": {
    "recurring_tests": {
     "frequency": "daily"
    },
    "pull_requests": {}
   },
   "build_args": {
```

```
    "root_workspace": "."
   }
  },
 "relationships": {
  "organization": {
   "data": {
    "type": "org",
    "id": "8f793725-eddf-4c7b-81e7-aa8546bd7df9"
   },
   "links": {
    "related": "/rest/orgs/8f793725-eddf-4c7b-81e7-aa8546bd7df9"
   }
  },
  "target": {
   "data": {
    "id": "3f997c18-0004-49a7-83f7-1b518b49d996",
    "type": "target",
    "attributes": {
     "display_name": "mnichols-snyk/strapi",
     "url": "https://github.com/mnichols-snyk/strapi"
    },
    "meta": {
     "integration_data": {
      "id": 891598420,
      "name": "strapi",
      "owner": "mnichols-snyk"
     }
    }
   },
   "links": {
```

```
      "related": "/rest/orgs/8f793725-eddf-4c7b-81e7-aa8546bd7df9/targets/3f997c18-0004-49a7-83f7-1b518b49d996"
     }
    },
    "importer": {
     "data": {
      "type": "user",
      "id": "ae8daca3-9df9-4275-b6dc-a3260a804aa3"
     },
     "links": {
      "related": "/rest/orgs/8f793725-eddf-4c7b-81e7-aa8546bd7df9/users/ae8daca3-9df9-4275-b6dc-a3260a804aa3"
     }
    }
   },
   "source_app_id": "50f158ef-6a8c-4c51-830c-baf16ed5d5a8",
   "name": "mnichols-snyk/strapi:package.json",
   "short_description": "Lifecycle:\nEnvironment:",
   "correlation_id": "mnichols-snyk/strapi",
   "last_policy_compliance_check_date": "NULL"
}
```


Example Usecase

To match **Container Repository Entries** with **Projects** based on Repository URL with name of CI.

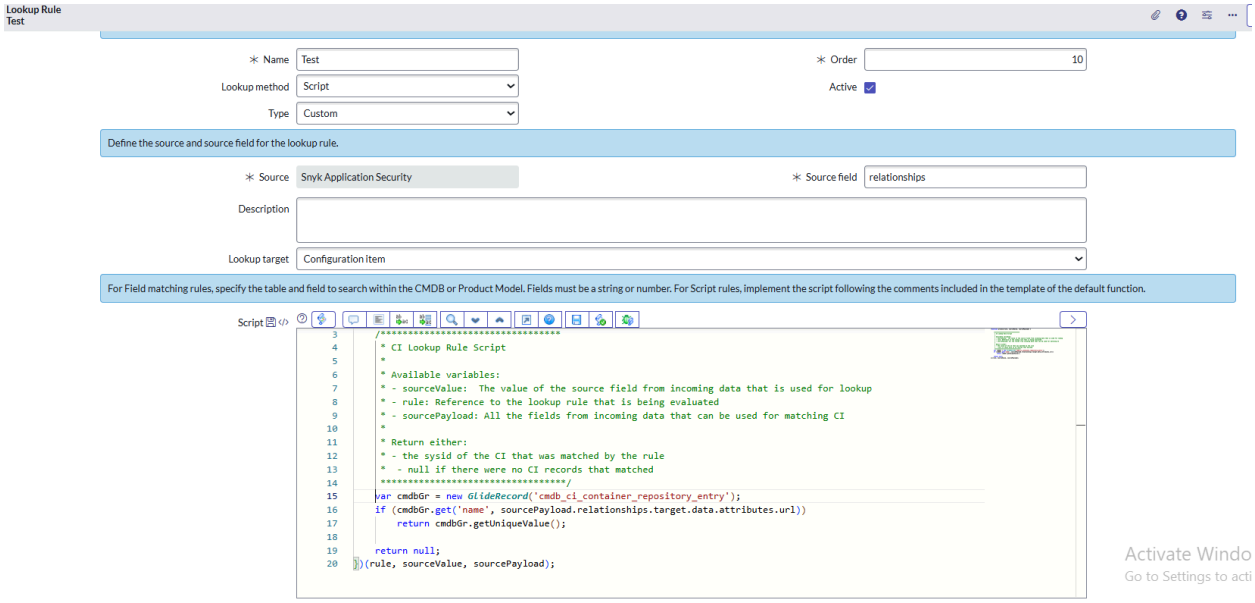
Create a Lookup rule with Lookup method as Script, type as Custom and Select Parent attribute if field is nested like in this example url is nested as `relationships.target.data.attributes.url`.

Below is screenshot of CI Lookup Record.

Script:

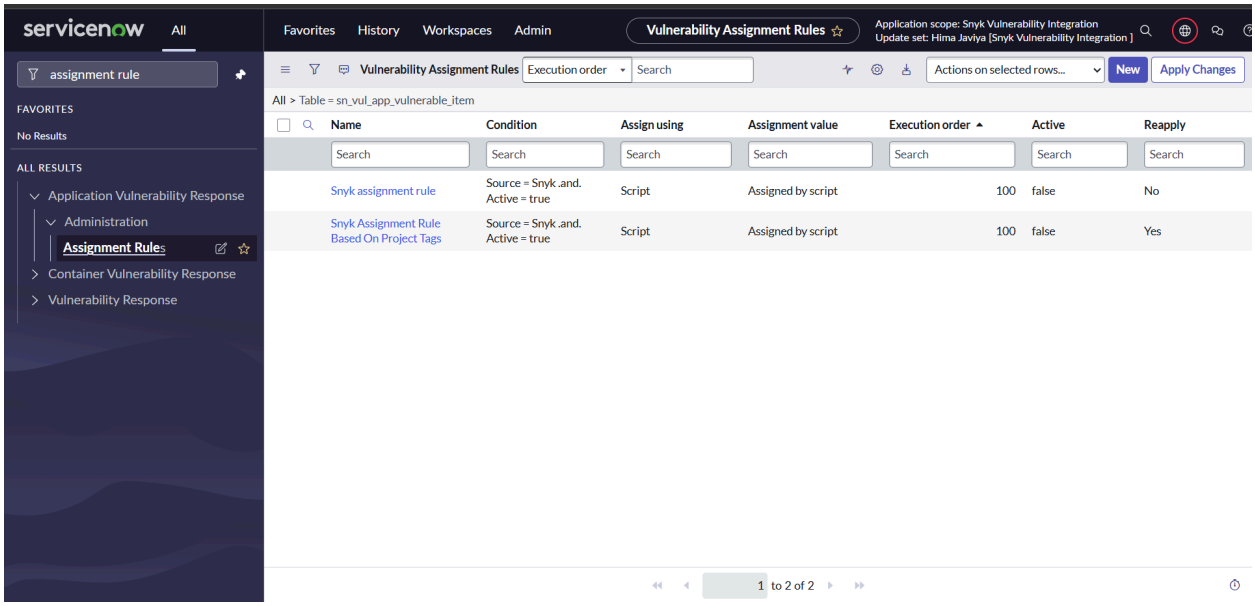
```
var cmdbGr = new GlideRecord('cmdb_ci_container_repository_entry');

    if (cmdbGr.get('name',
sourcePayload.relationships.target.data.attributes.url))

        return cmdbGr.getUniqueValue();
```

```
    return null;
```



4.14. Assignment Rule

- The Snyk application has two assignment rules by default in an inactive state: 1) Snyk Assignment Rule and 2) Snyk Assignment Rule Based On Project Tags for assigning AVIT to users/groups.
- **Navigate to Application Vulnerability Response > Administration > Assignment Rules for more information.**

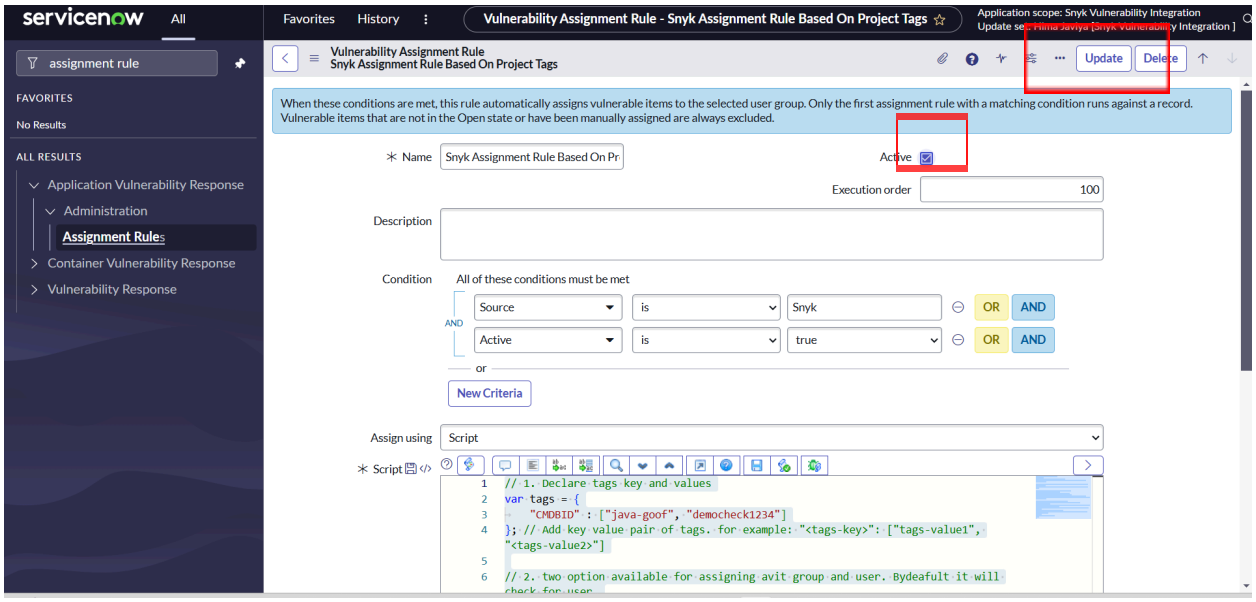


1. **Snyk Assignment Rule Based On Project Tags**
   a. If you want to assign AVIT based on project tags, use this assignment rule. To use this assignment rule, you need to make below changes.

```
// 1. Declare tags key and values
var tags = {
    "CMDBID" : ["java-goof", "democheck1234"]
}; // Add key value pair of tags. for example:
"<tags-key>": ["tags-value1", "<tags-value2>"]

// 2. two option available for assigning avit group and
user. By default it will check for user.
var whomToAssign = "user";  // Replace with group if
you want to assign AVIT to group

// 3. Mapping of tags value and sys id of user/group.
var sysIdOfUserOrGroupBasedOnTags = {
    "java-goof": "afdf1ee287d9421015f3c91e0ebb357a",
    "democheck1234": "afdf1ee287d9421015f3c91e0ebb357a"
}; // If you want to assign user to AVIT which has
<tag-value> in discovered application/projects. then
delcare it in above dict like "<tag-value>"" : "<sys-id
of user/group>"

// 4. Logic to map appropriate user/group to AVIT
```

```
var sourceDict =
current.application_release.source_additional_info;
for (var key in tags){
    if (sourceDict[key] !== undefined &&
tags[key].indexOf(sourceDict[key]) != -1){
        if (whomToAssign == "user"){
            current.assigned_to =
sysIdOfUserOrGroupBasedOnTags[sourceDict[key]];
        }
        else if (whomToAssign == "group"){
            current.assignment_group =
sysIdOfUserOrGroupBasedOnTags[sourceDict[key]];
        }
        break; // match found
    }
}
```

b. Check comments in the code and update the codebase accordingly so it works seamlessly with your data and mark it as active.

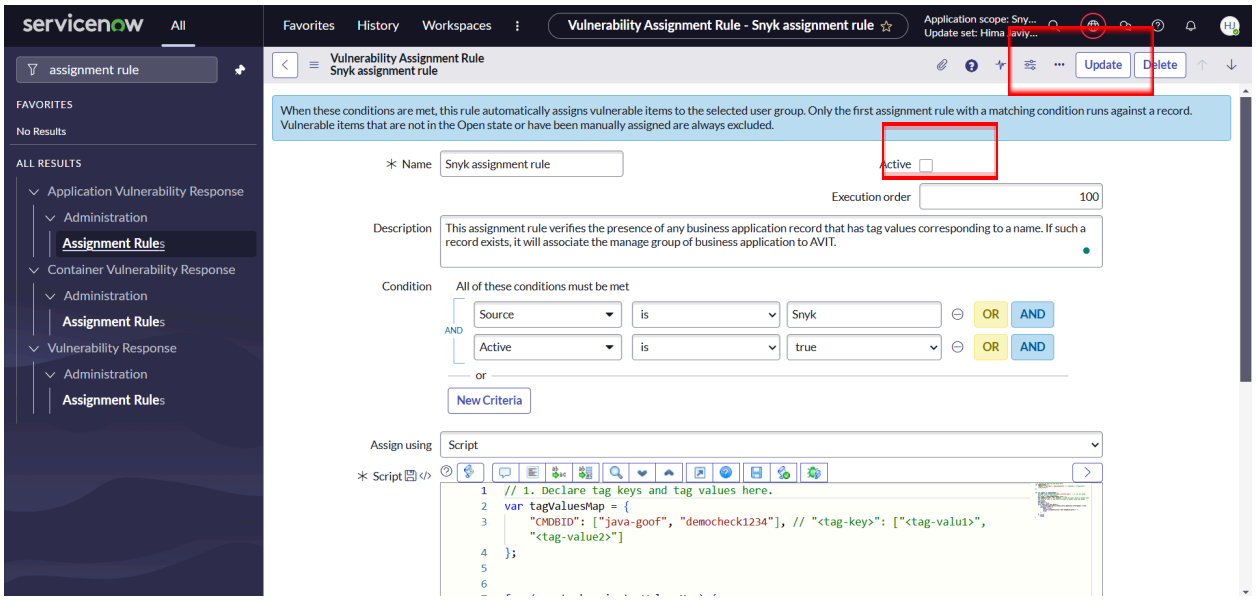


2. Snyk assignment rule

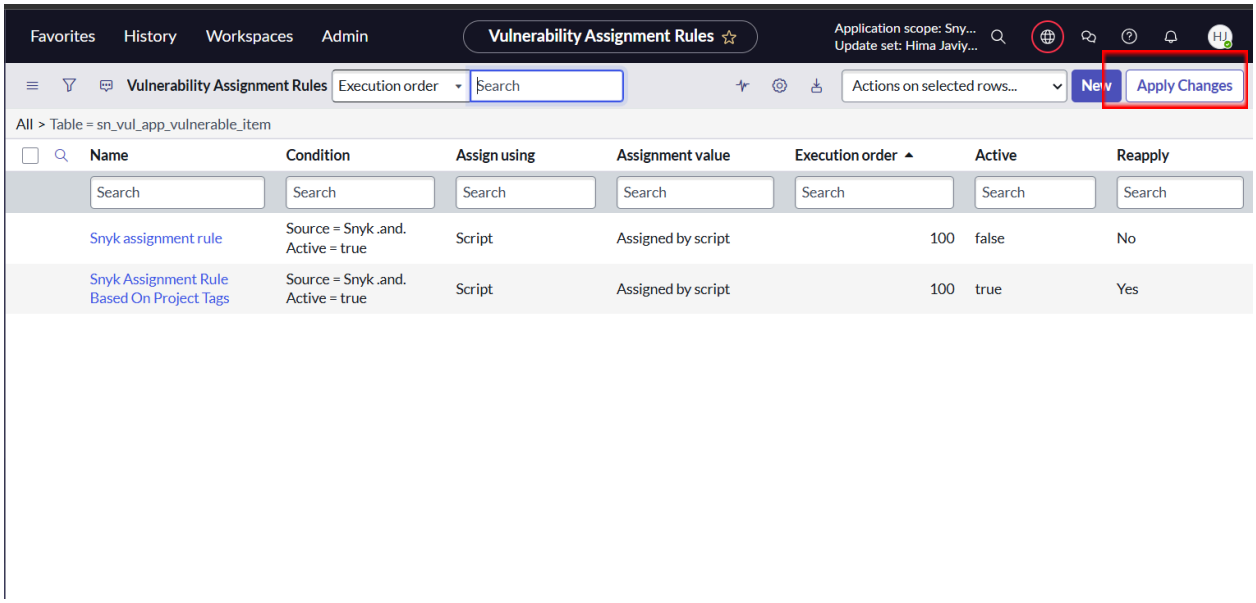
a. This assignment rule verifies the presence of any business application record with tag values corresponding to a Business App name. If such a record exists, it will associate the managed by group of the business application to the AVIT. Change the code below according to your requirements.

```
// 1. Declare tag keys and tag values here.
var tagValuesMap = {
    "CMDBID": ["java-goof", "democheck1234"], //
"<tag-key>": ["<tag-valu1>", "<tag-value2>"]
};


for (var tagkey in tagValuesMap) {
    var baGr = new GlideRecord("cmdb_ci_business_app");
// 2. you can change table as per your requirements
    var values = tagValuesMap[tagkey].join(",");
    baGr.addQuery("name", "IN", values);  // Make sure
your record is present with tag values as name. If tag
value is present in another field then change
accordingly.
    baGr.query();
    var match = false;
    while (baGr.next() && !match) {
        if
(current.application_release.source_additional_info[tag
key] == baGr.getValue("name")) {
            match = true;
            current.assignment_group =
baGr.managed_by_group + "";
            break;
        }
    }
    if (match)
        break;
}
```

b. Change the tag key and tag values according to your environment and check other comments. After changing, mark active as true for this assignment rule.

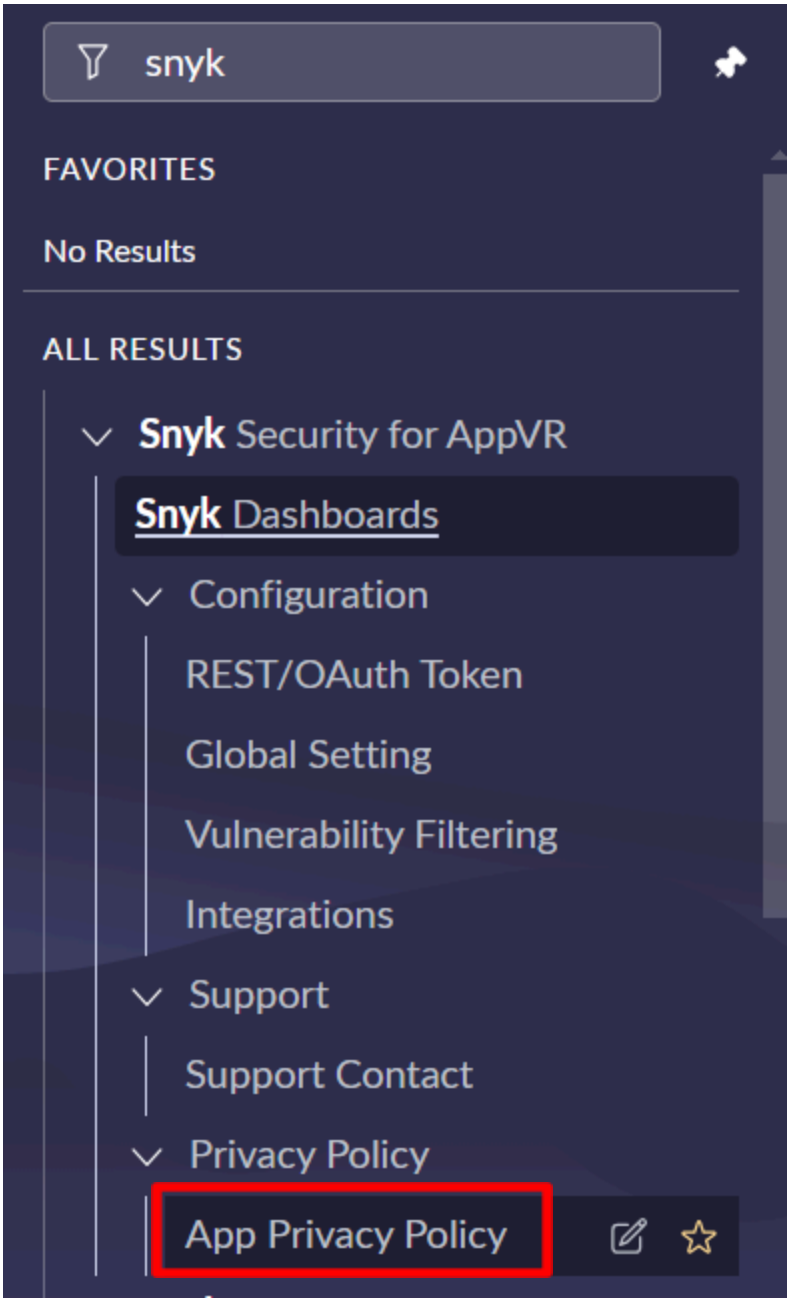


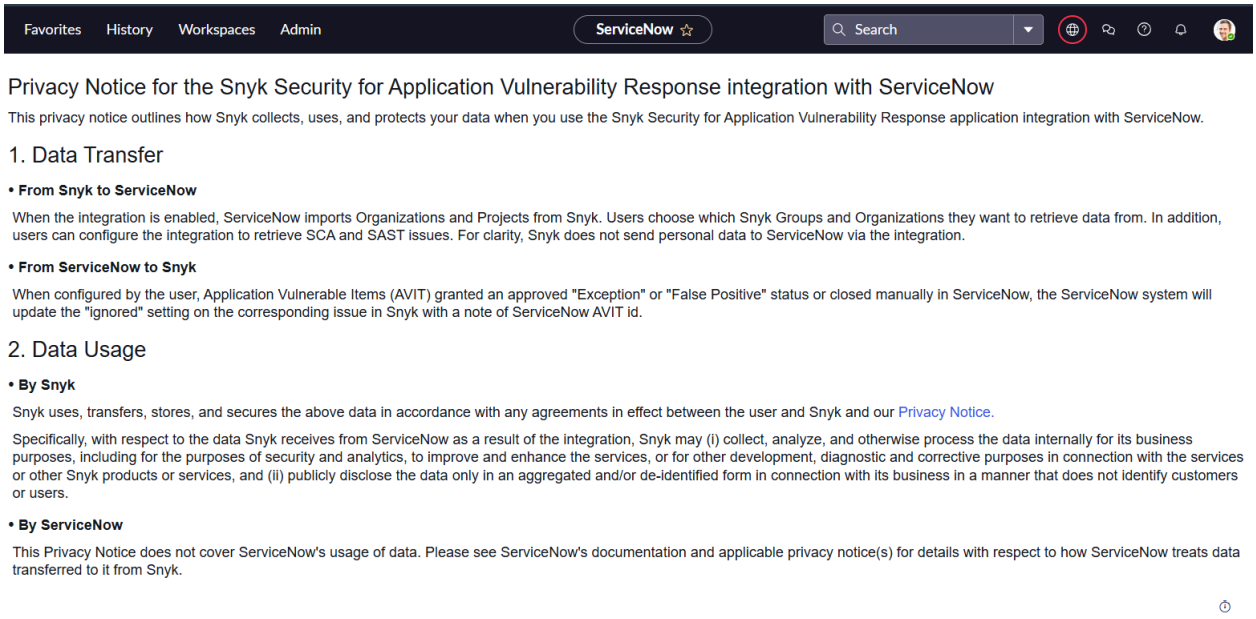
c. Apply the changes to run the assignment rule for existing AVITs.



4.15. Privacy Policy

- Navigate to "Snyk Security for AppVR."
- To check the privacy policy related to the application, navigate to "Snyk Security for AppVR," and under it, look for "Privacy policy" and select "App Privacy Policy" from the dropdown menu.

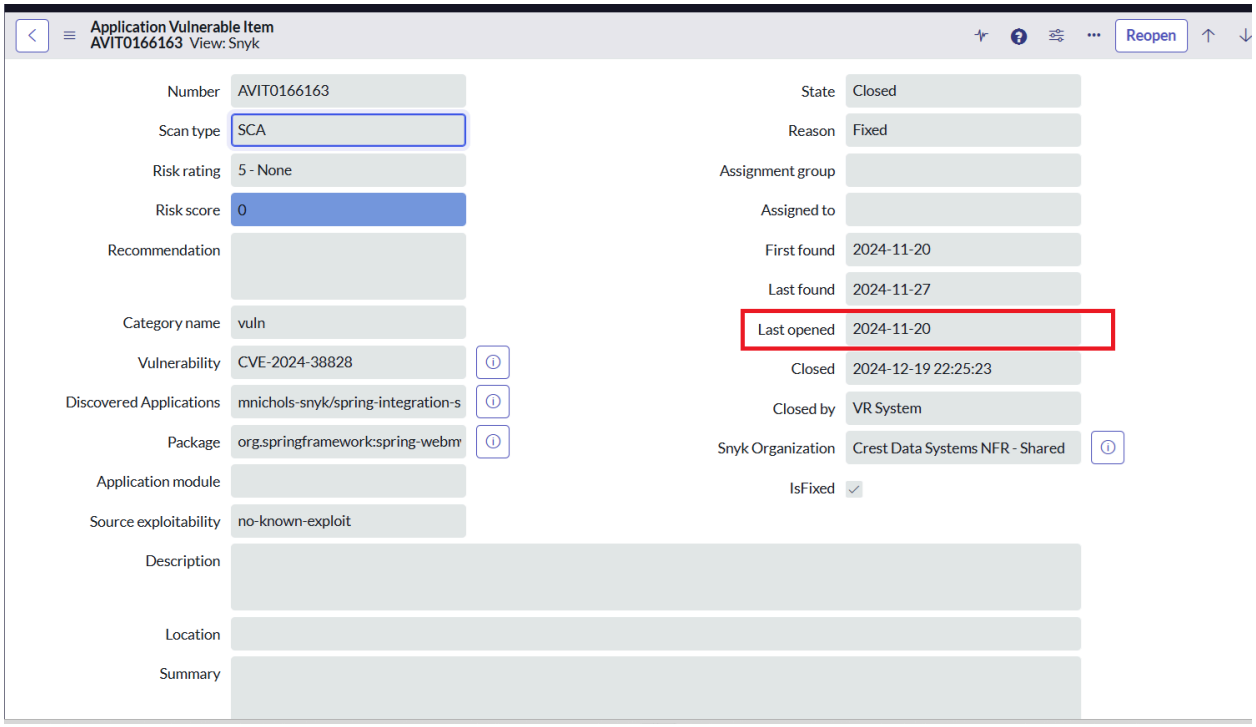

snyk
FAVORITES
No Results
ALL RESULTS
Snyk Security for AppVR
Snyk Dashboards
Configuration
REST/OAuth Token
Global Setting
Vulnerability Filtering
Integrations
Support
Support Contact
Privacy Policy
App Privacy Policy



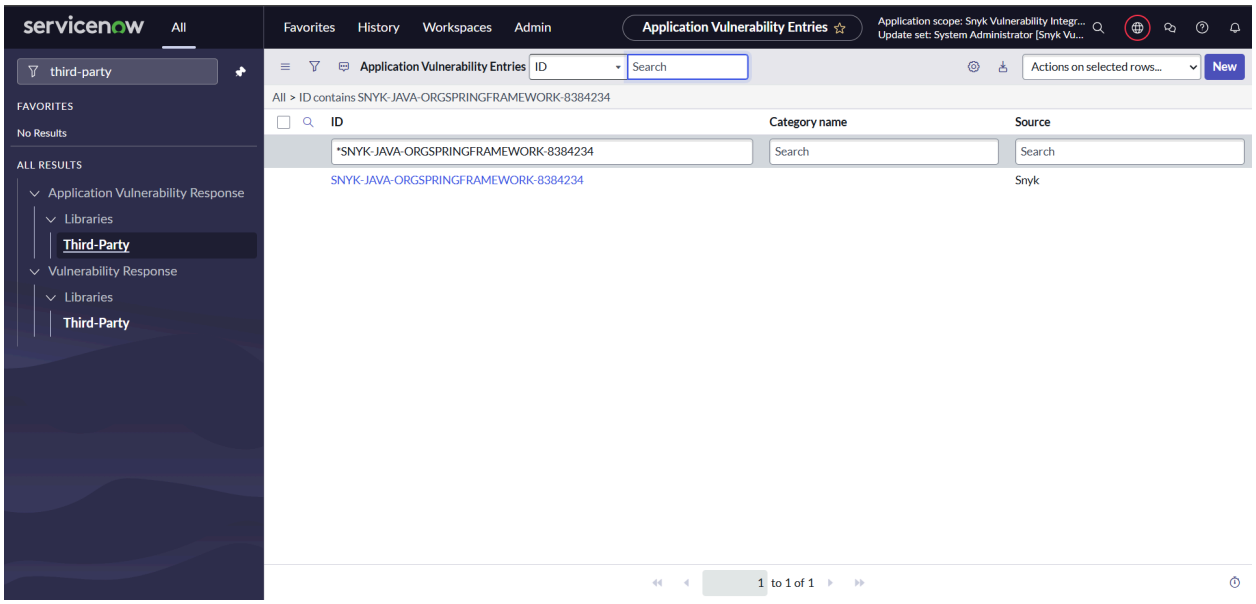
5. Upgrade Behaviour (From 3.0.0)

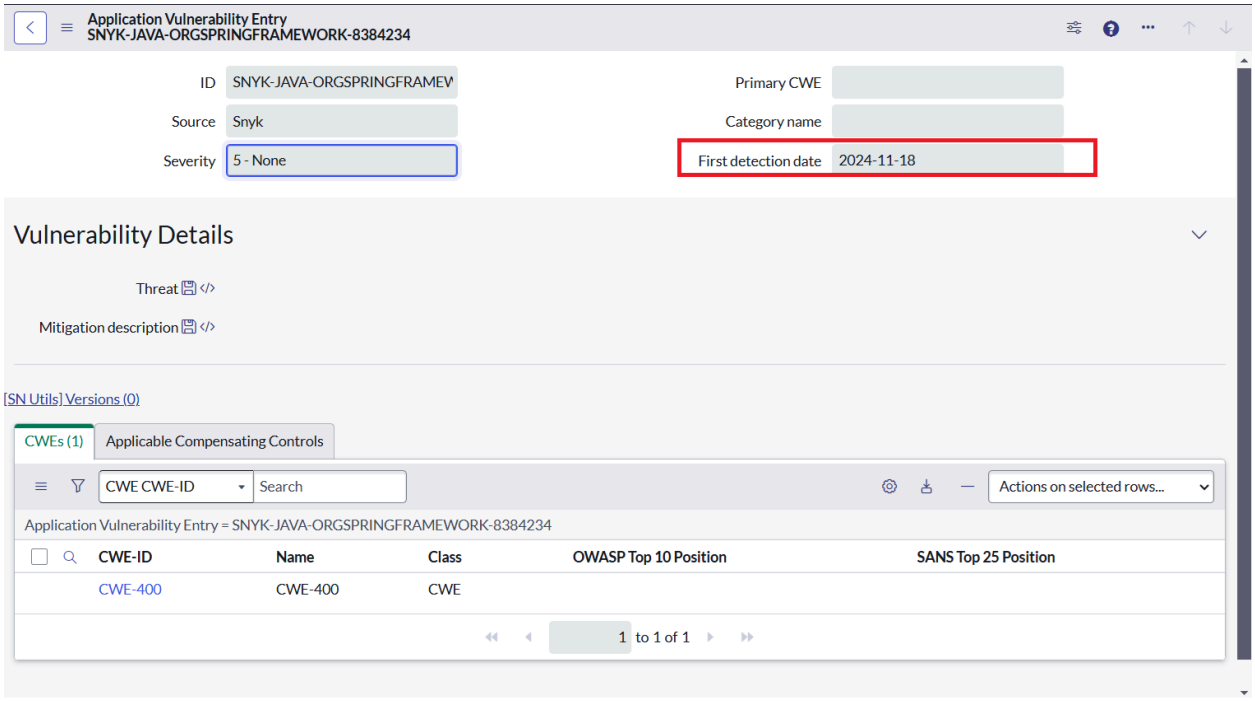
5.1. Changed mapping of last opened in AVIT

- In previous versions, the "disclosure Time" of SCA issues was mapped to the "last opened" field of an AVIT. That behavior is now changed to "First detection date" in the third-party table as it is a more logical mapping for the integration.
- To see the "disclosure time" in ServiceNow, navigate to Application Vulnerable Items.
- Open any SCA AVIT that is fetched from V1 integration.



- Now copy the Source AVIT ID of the same AVIT. (Exclude content after pipe(| for example, if Source AVIT ID is SNYK-JAVA-ORGSPRINGFRAMEWORK-8384234 | CVE-2024-38828, then copy only SNYK-JAVA-ORGSPRINGFRAMEWORK-8384234).
- Now Navigate to Third-party.
- Search with copied ID.

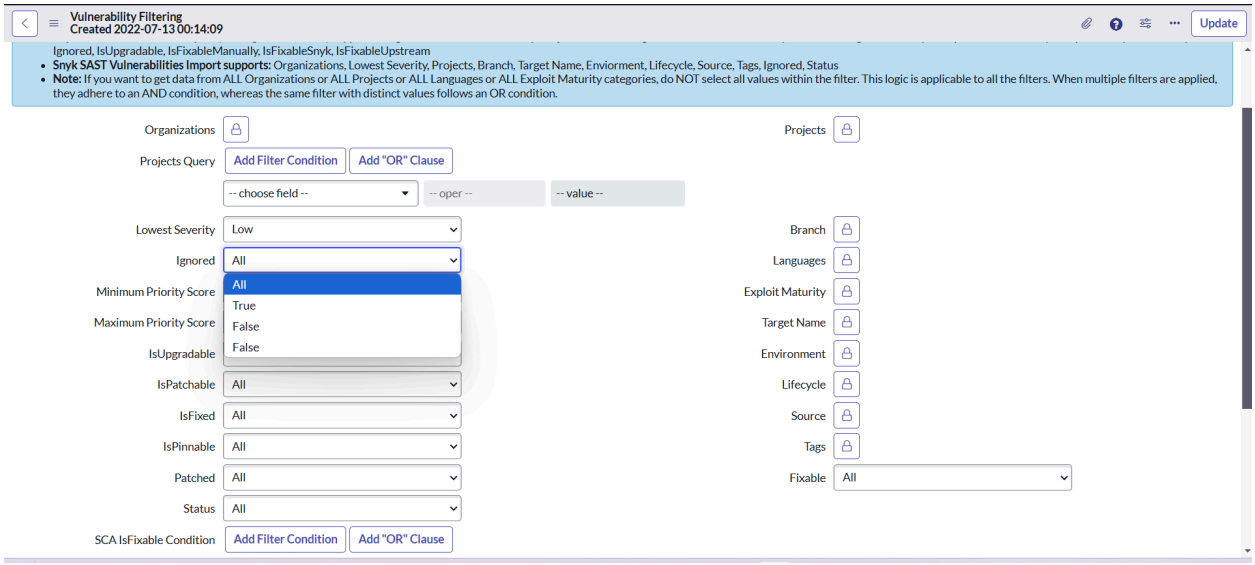




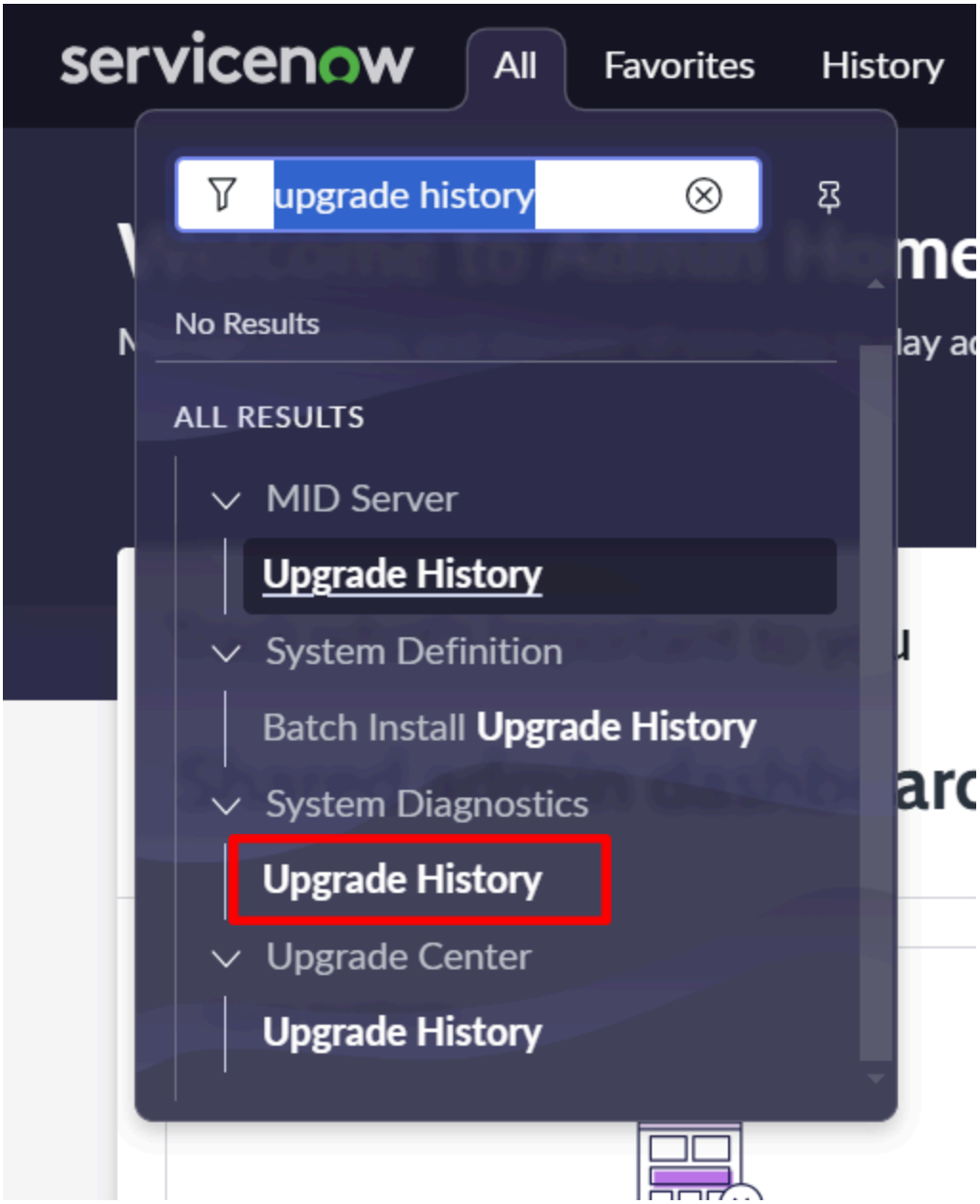
- Note: If the user has created a dashboard, assignment rule, etc., on the "last opened" field, then going forward, the user needs to use the "First detection" date of the Third-Party Entry table to get the same results.

5.2. Two false options in Vulnerability filtering (Perform the steps below to remove duplicate options)

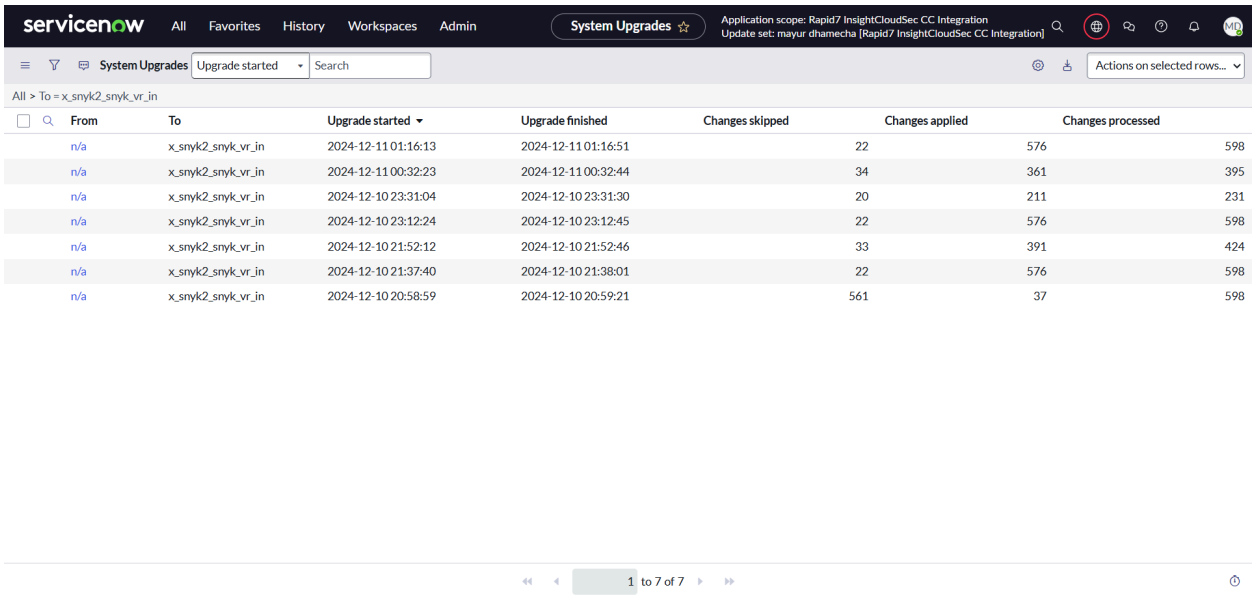
Note: This will only apply if a user sees multiple false values on the vulnerability filtering page. Refer to the screenshot below for more details.



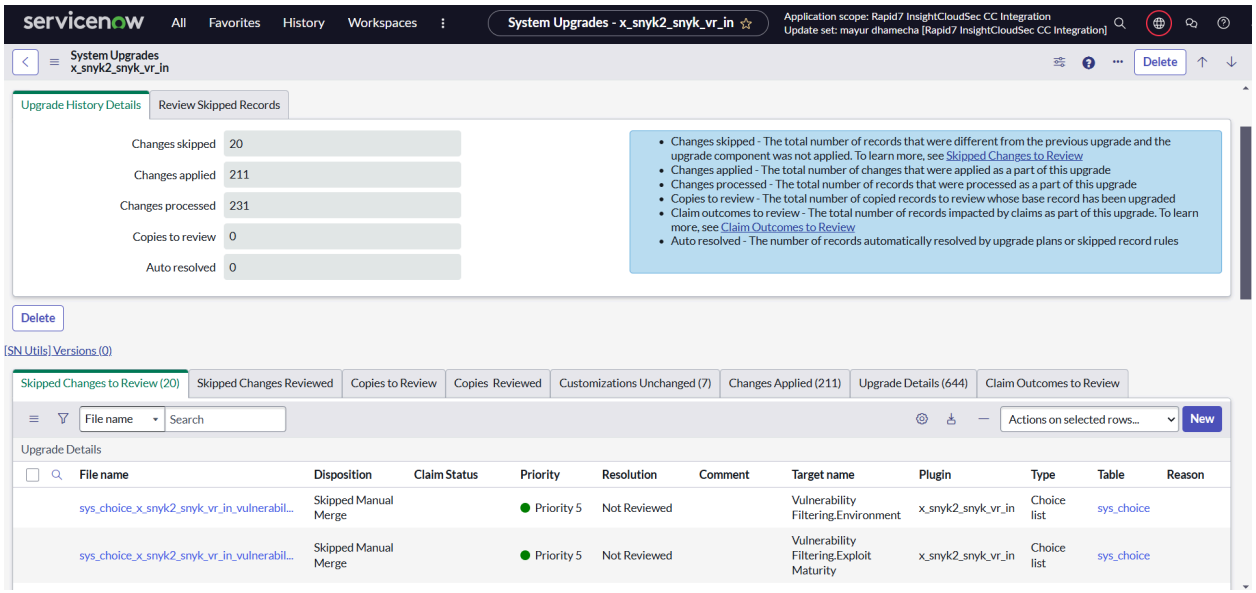
- Navigate to System Diagnostic > Upgrade History.



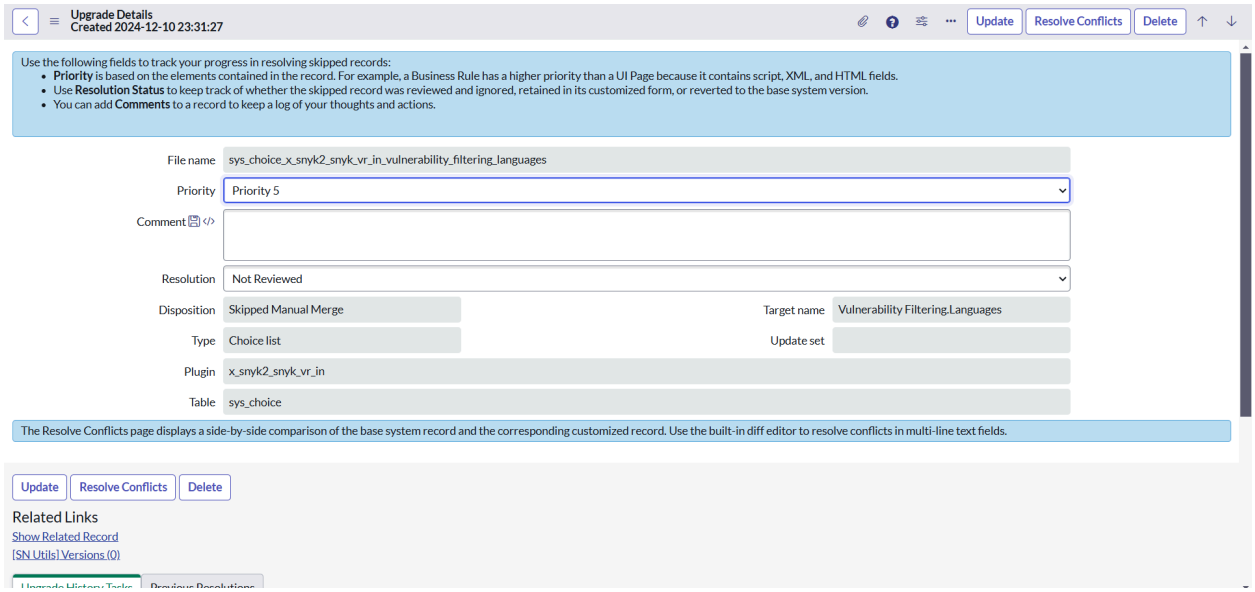
- Search with To=x_snyk2_snyk_vr_in and Sorted in descending order with the field Upgrade started.



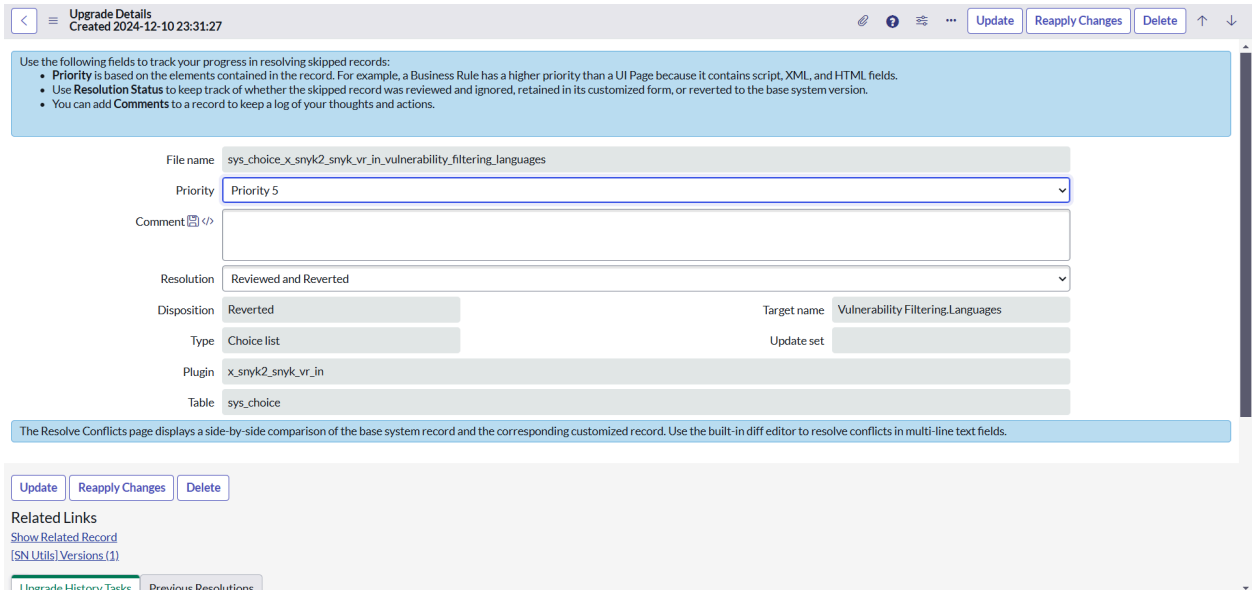
- Open the first record.
- Review the Skipped Changes to Review with a Disposition as Skipped Manual Merge.



- Open every record and do the following.
- Click on Resolve Conflicts



- Click on Revert to Base System.



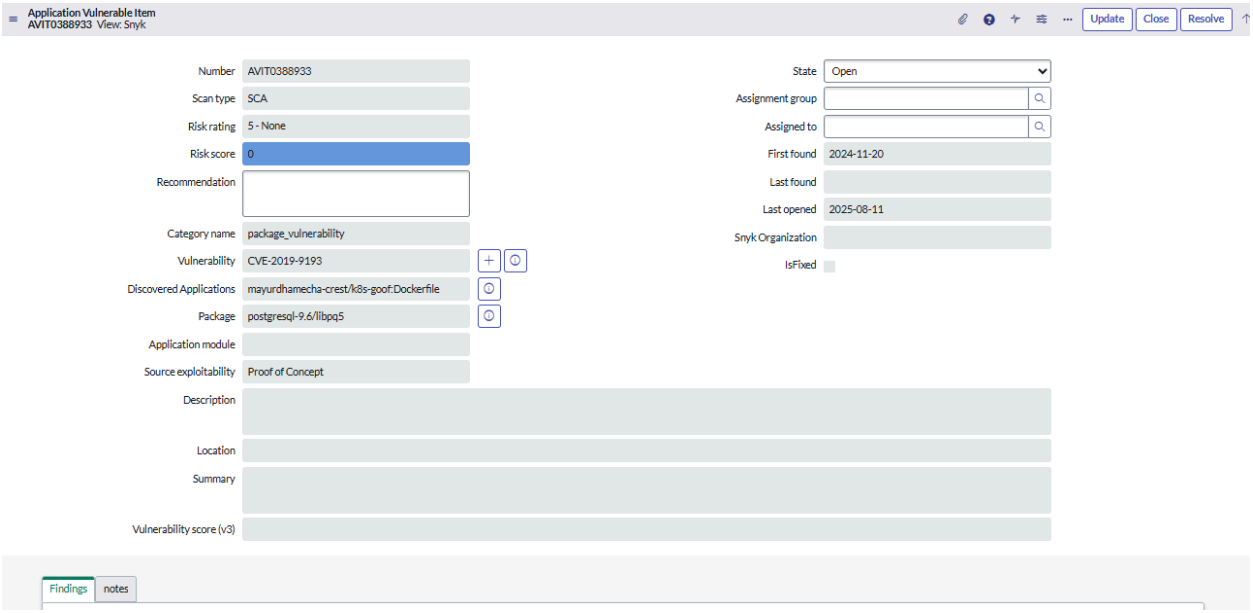
- Do the same for the remaining record.
- Alternatively, the user can run the script below in "script - background" (Global Scope) to remove duplicate choices.

```
ar choiceGr = new GlideRecord("sys_choice");
choiceGr.addEncodedQuery("name=x_snyk2_snyk_vr_in_vulnerability_filtering^element=fixable^ORelement=ignored^ORelement=isfixed^ORelement=is_fixed^ORelement=is_patchable^ORelement=is_upgradable^ORelement=patched^ORelement=is_pinnable^valueISEMPTY");
choiceGr.query();
choiceGr.deleteMultiple();

choiceGr = new GlideRecord("sys_choice");
choiceGr.addEncodedQuery("name=x_snyk2_snyk_vr_in_fixable_filters^element=is_fixable_upstream^ORelement=is_fixable_manually^ORelement=is_fixable_snyk^valueISEMPTY");
choiceGr.query();
choiceGr.deleteMultiple();
```

6. Upgrade Behaviour (From 3.1.0)

6.1. Changed mapping of Source exploitability in AVIT

- In previous versions, the source exploitability field wasn't mapped for the AVITs fetched using Integration - Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API).
- To see the "Source exploitability" in ServiceNow, navigate to Application Vulnerable Items.
- Open any SCA AVIT that is fetched from REST integration.

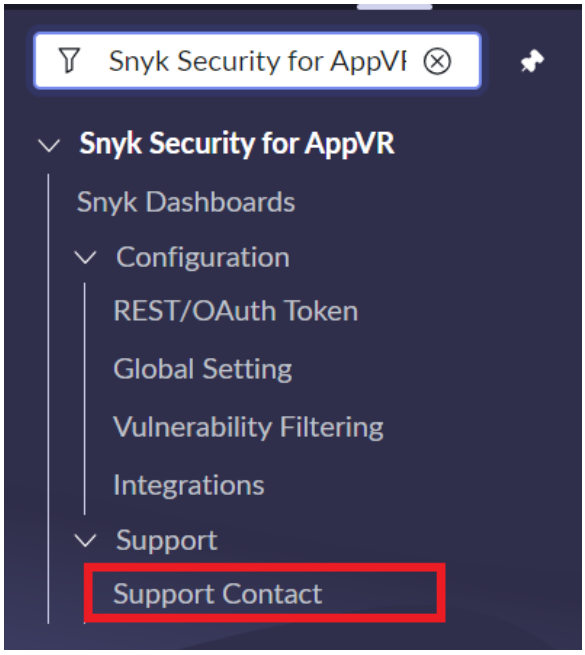


- The Source exploitability field is now mapped to the CVSSv4 value. If CVSSv4 is not available for that vulnerability, the CVSSv3 value will be used instead.
- Note: To map this field for existing records, clear the Start Time of the integration Snyk SCA & IaC Vulnerabilities Import (All Regions – REST API) and execute the integration again.

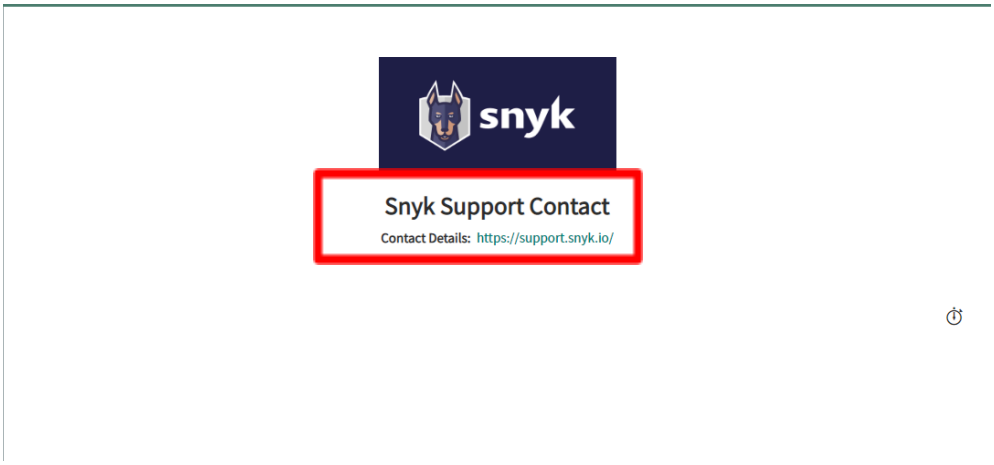
7. Support, Troubleshooting, and Known Behaviors

7.1. Support

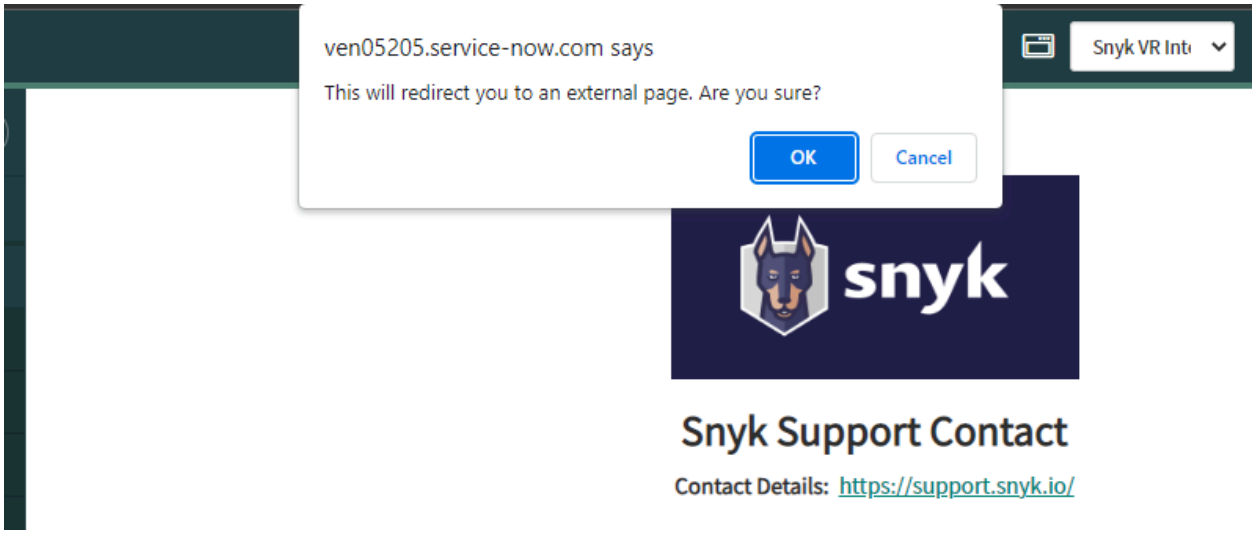
- Navigate to "Snyk Security for AppVR."
- For any issues related to the application, navigate to "Snyk Security for AppVR," and under it look for "Support" and select "Support Contact" from the dropdown menu.



- Support Contact opens with the Snyk support URL.



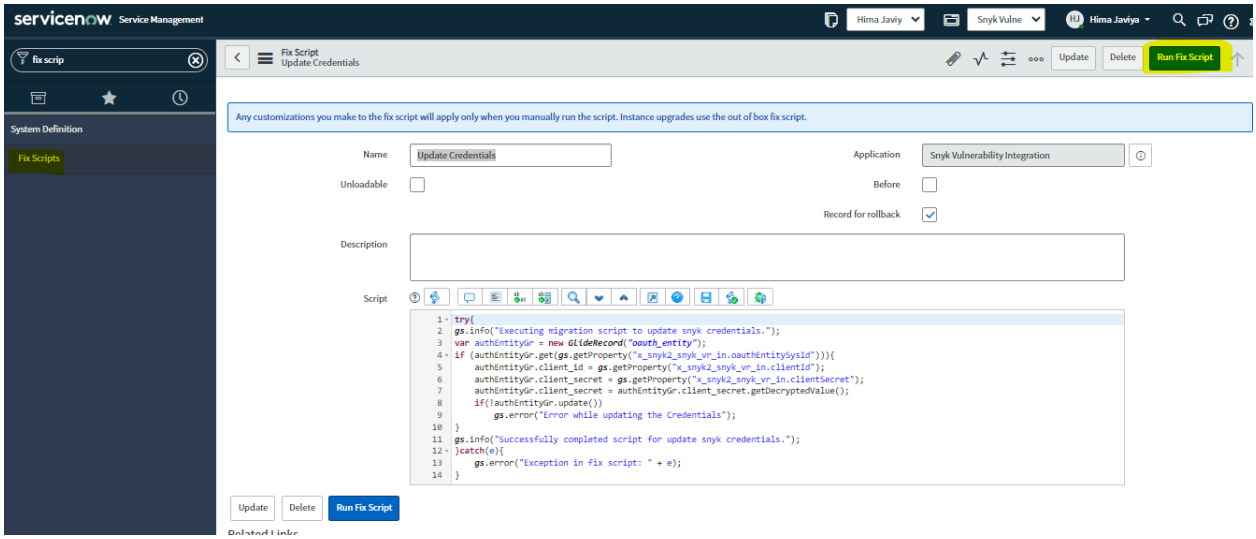
- Click on the contact detail links, which opens a pop-up with the message "You will be redirected to an external website. Are you sure?" Click on "OK" to open the link.



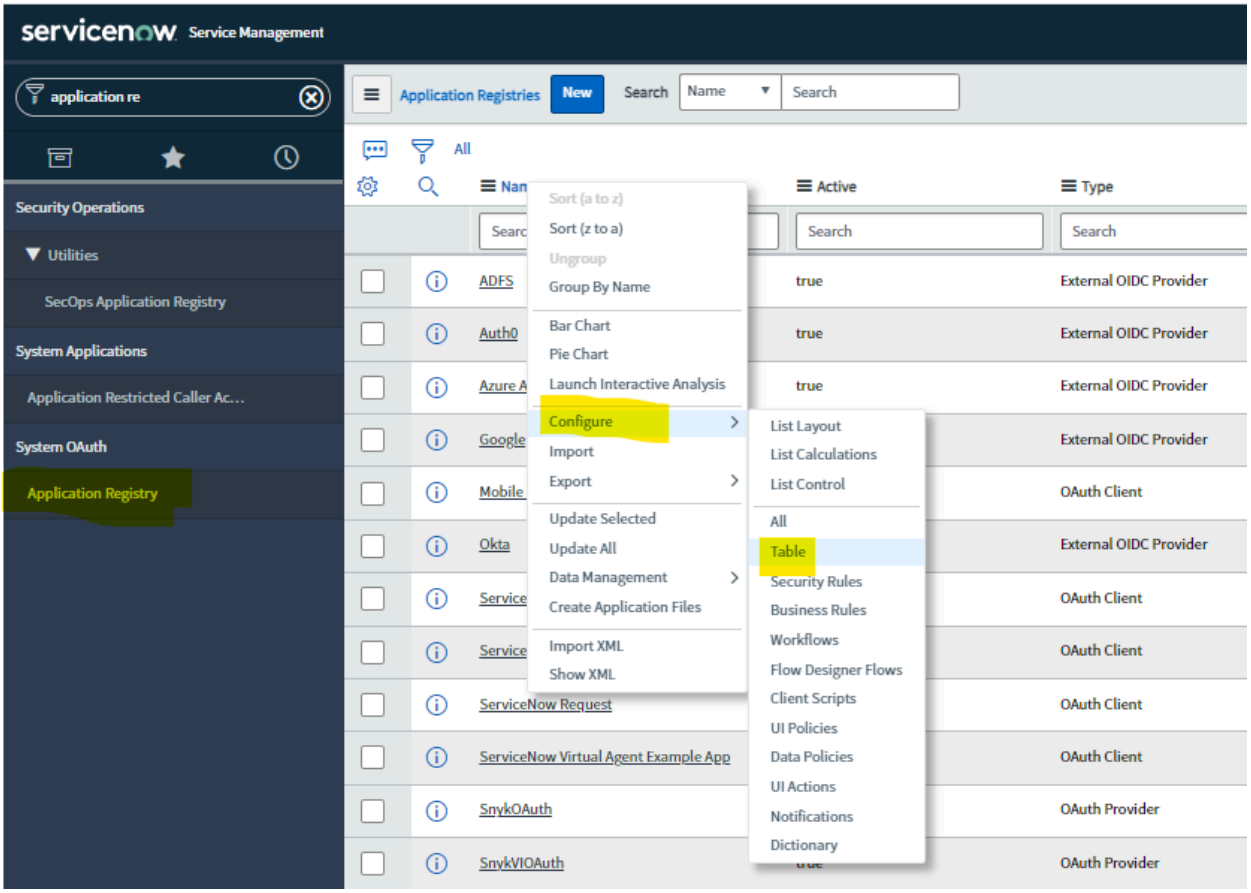
7.2. Troubleshooting

7.2.1. Unable to generate the token

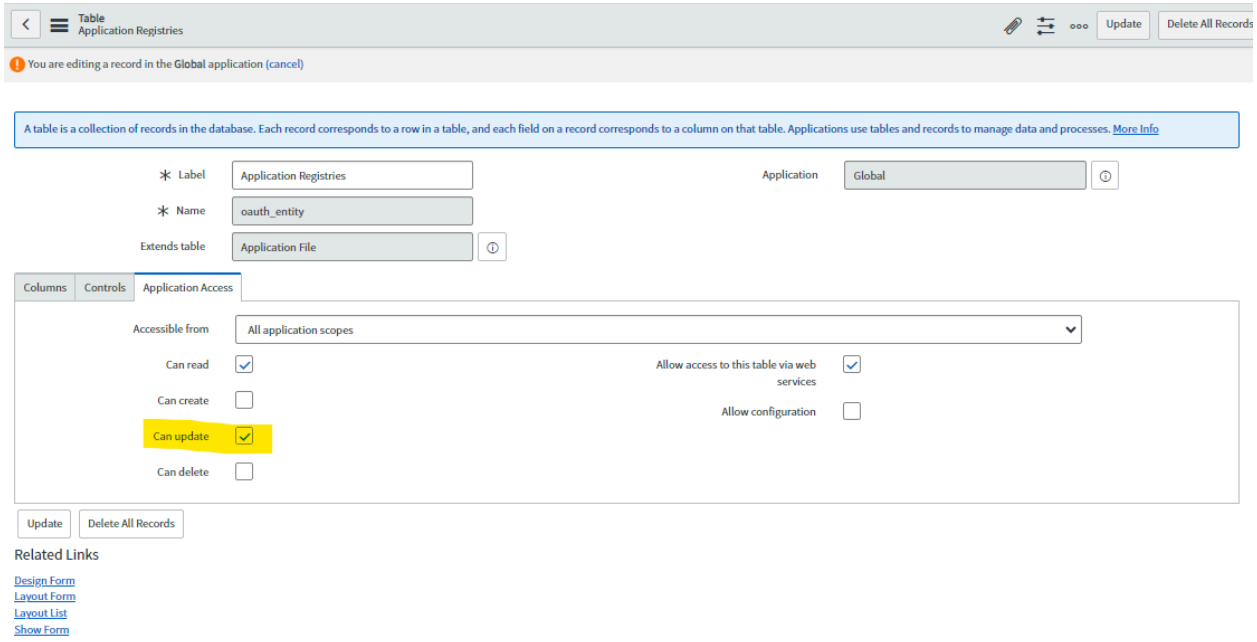
- Navigate to Fix script under system definition from the navigation module.
- Search "Update Credentials" in the name.
- Open the record and click on "Execute Now."



- Now, try to generate the token again. It should be generated successfully.
- If you still face an error in token generation, follow the steps below.
- Navigate to Application Registry under System OAuth.
- Right-click on the header of the table column and open Configure > Table.



- Check the "Can Update" checkbox under application access. Mark it true and save the record.
- Run the "Update Credentials" fix script again.
- Generate the token. It should be generated successfully.



7.2.2. Unable to install "Snyk VR Integration" from the ServiceNow Store

- Verify you have the role of system administrator (admin).
- Navigate to "System Definition" and select "All" from the dropdown menu in your instance.
- Verify whether the following application has been installed or not. If not, then first install this application.

7.2.3. Unable to create a new user

- Review the following link and execute the steps.

  https://www.servicenow.com/docs/bundle/washingtondc-customer-service-management/page/administer/users-and-groups/task/t_CreateAUser.html

7.2.4. Unable to install/activate the plugin in ServiceNow Instance

- Review the following link and execute the steps.

  https://docs.servicenow.com/bundle/xanadu-platform-administration/page/administer/plugins/task/t_ActivateAPlugin.html

7.2.5. The user deletes the Application Registry default record

- Uninstall the application and reinstall the application.

7.2.6. The user deletes the REST Message default record

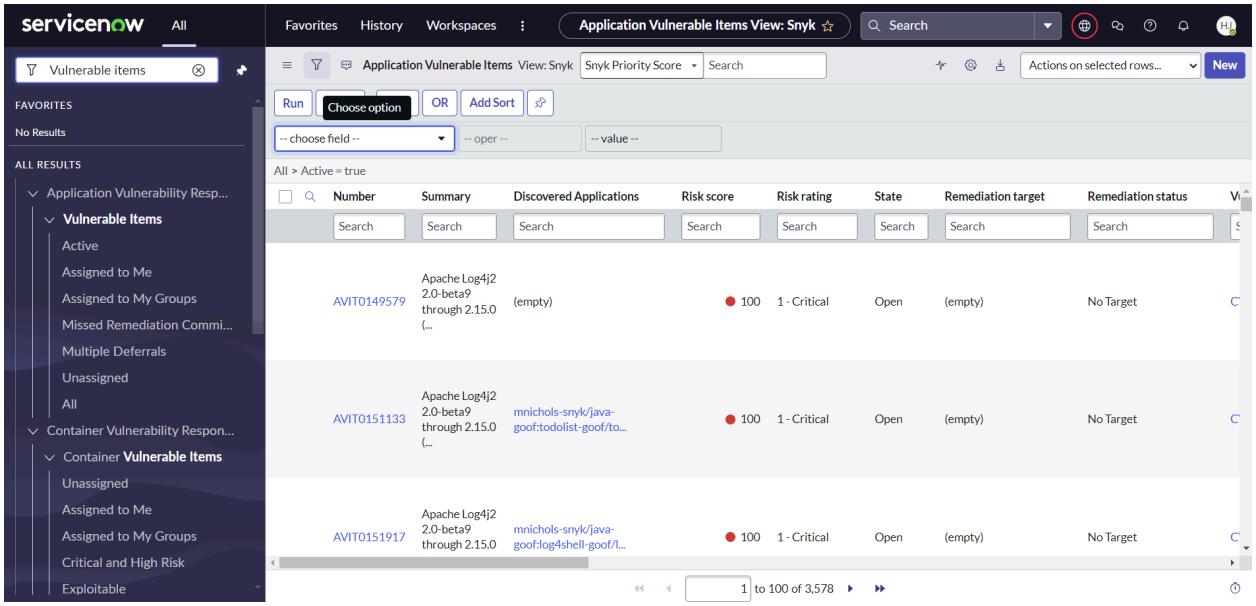
- Uninstall the application and reinstall the application.

7.2.7. The user deletes any of the Integrations records

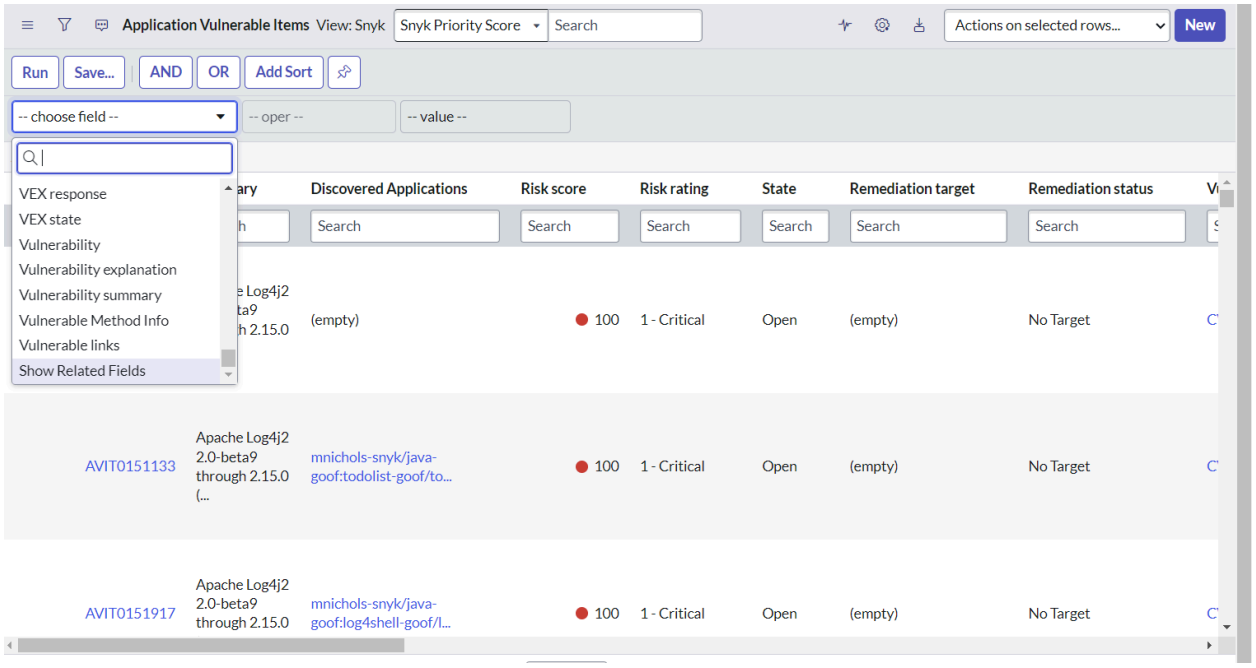
- Uninstall the application and reinstall the application.

7.2.8. Unable to search Lifecycle & Environment from AVIT

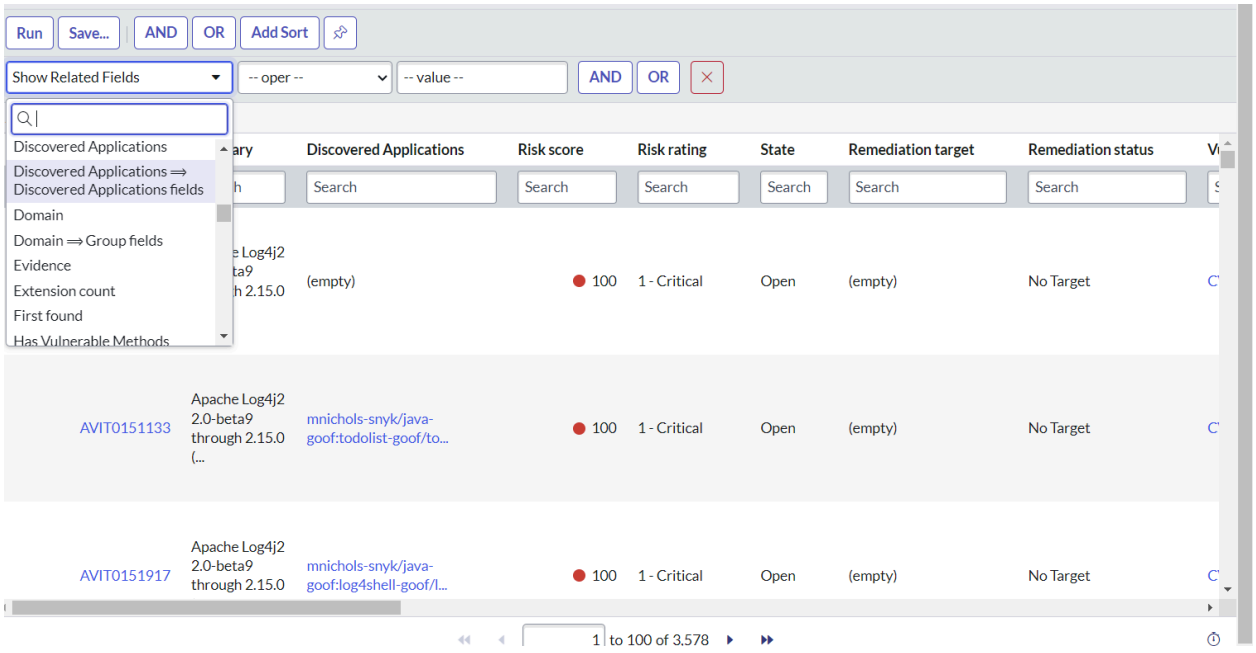
- Navigate to Application Vulnerable items.
- Click on the Show/Hide Filter icon from the top.



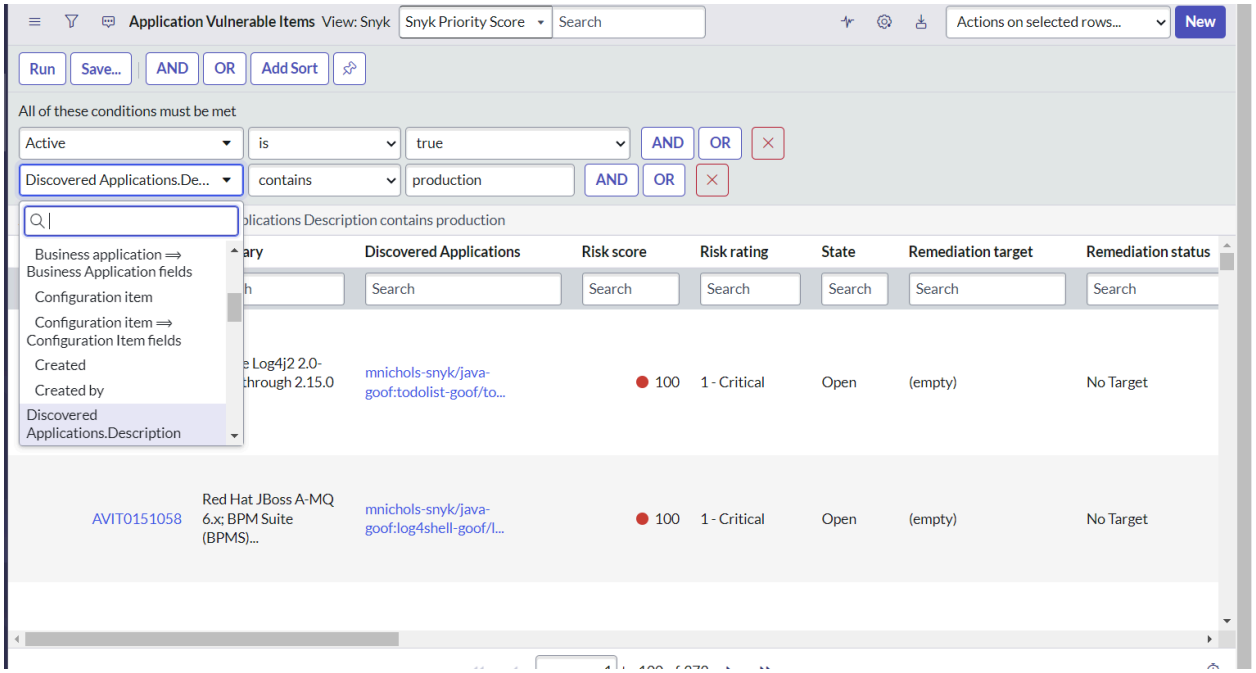
- Click on the dropdown and select Show Related Fields.



- Again, open the dropdown and select the Discovered Application > Discovered Application fields.



- Now again, open the dropdown and select the Description.



7.2.9. Unable to see CVE & CWE in the Third-party records

- Open Application Vulnerability Response> Libraries> Third-Party, Open the third-party record.
- Click on Additional Action > Configure> Related Lists. The form will open. Add the CVE & CWE to the selected list and click save.

7.2.10. Organizations were not found, or you do not have permission to access them

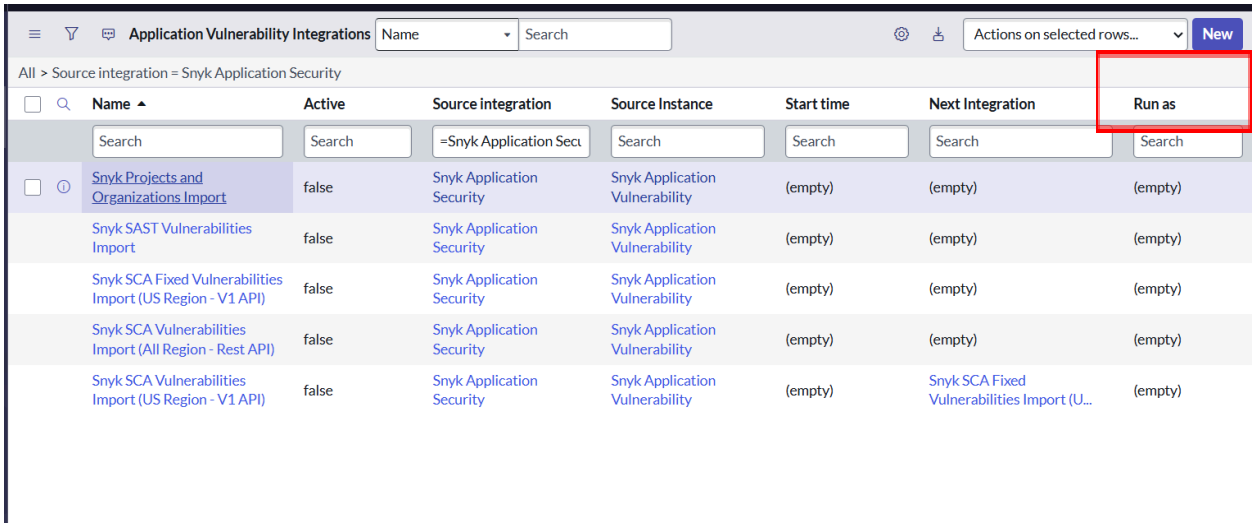
- Snyk Apps can only be authorized for a single org or all orgs in a group. If you attempt to authorize for multiple orgs (without using All Orgs), the authorization will only be for the last Org authorized.

7.2.11. Invalid Redirect URL error message while authorizing Snyk Application

- The user must ensure that the instance redirect URL (i.e., https://YOUR-INSTANCE.service-now.com/oauth_redirect.do) is provided to the Snyk team through email (servicenow@snyk.io).

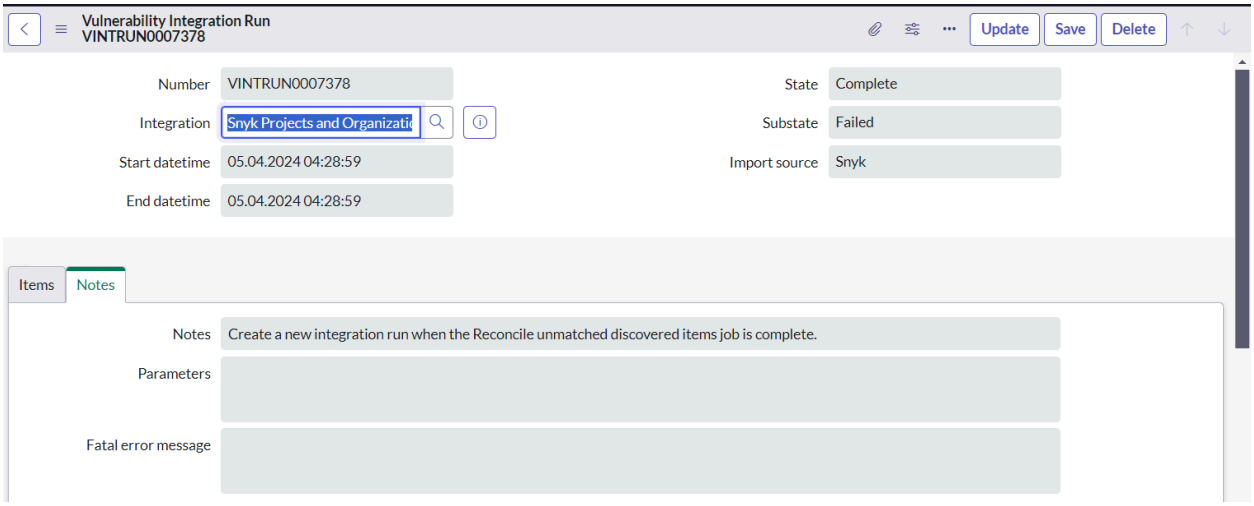
7.2.12. Able to generate the token, but integration is failing.

- The integration run fails if a value is assigned in the **Run as** field in the integration configuration. Make sure that you keep it empty for all the integrations.



7.2.13. Getting Reconcile-related errors while running integration.

- This error occurs when multiple VR integrations are running on the same instance.
- Follow the steps below if you get this error while running Snyk integrations.



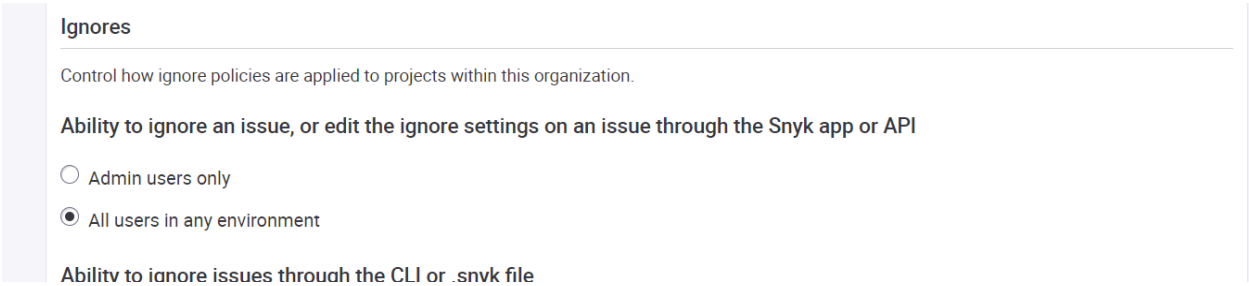
- Navigate to `sn_sec_cmn_background_job.list`
- Make sure all the listed job states are complete. If any job is not in a "complete" state and the job is important, wait for the background job to finish. If a background job is unimportant, mark it complete using the script below.
- If you can change the state of the job from the UI, then you can mark the job as completed. Otherwise, run the script below in scripts - Background while in the Global scope. You can copy the sys_id of jo by right-clicking on the record.

```
var gr = new GlideRecord("sn_sec_cmn_background_job");
if (gr.get("<sys_id of background job>")){
        gr.state = "complete";
        gr.update();
}
```

- Run the Snyk integration again.

7.2.14. Unable to ignore an issue from ServiceNow to Snyk. Getting 403 Error in Outbound HTTP Calls.

- Open the Snyk platform at the organization level. Go to Settings.



- In General settings, You must select "All users in any environment" to successfully ignore the issue.
- To restrict the ability of developers to ignore issues in Snyk without ignoring them in ServiceNow, a custom group role must be created in the Snyk UI at the Group level that

does not allow members of that group to ignore items. Then, developers who should not be allowed to add an ignore in Snyk must be added to that group. See this documentation from Snyk on how to create the custom roles: https://docs.snyk.io/snyk-admin/manage-permissions-and-roles/user-role-management.

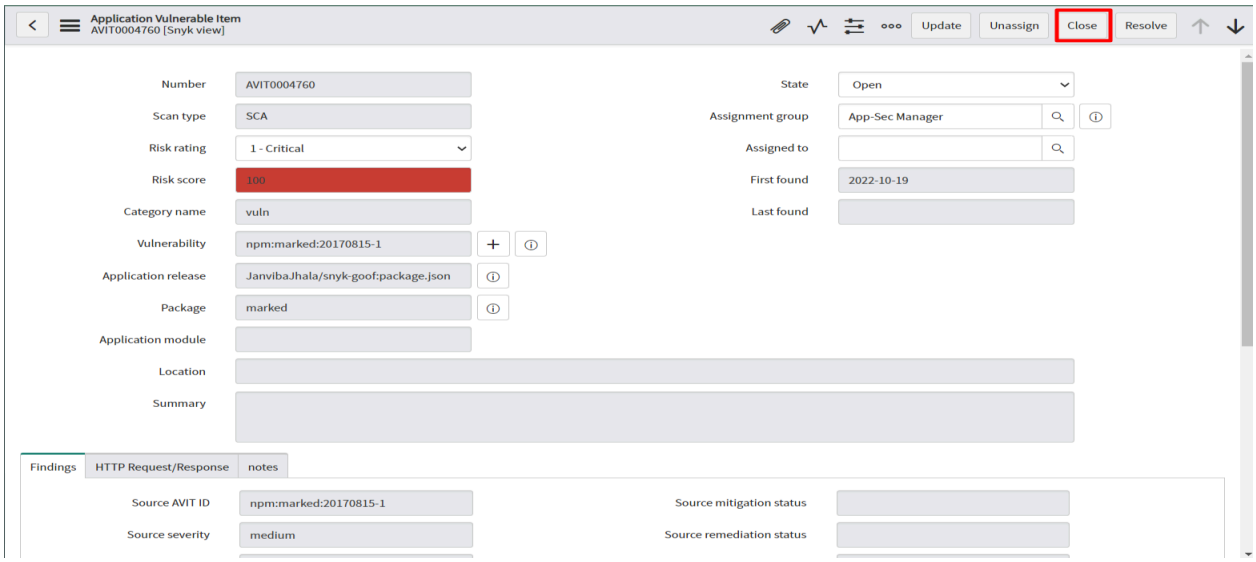
7.3. Known Behaviors

7.3.1. Vulnerability Integration fails when one integration is running and the second integration is executed.

- Snyk uses the ServiceNow default OAuth2 mechanism to manage tokens. The OAuth credentials table is only accessible by the token owner, a user with the "maint" role, or a system admin.
- Because of the limitations of the read ACL, the Snyk integration run fails when run as the user VR.system while a job with that user is still running.
- The vulnerability response scheduler runs the integration as a VR.system user when one job is already running and the second executes.
- To avoid this case, don't manually execute a Snyk import job when one run is already in process. If you want to run an integration job, then cancel the running integration run and retry.

7.3.2. The Snyk application vulnerable item is in the open state even if the Snyk issue is fixed in the Snyk platform.

- If the first ingestion of the Snyk issue does not contain CVEs, but the second ingestion of the same Snyk issue does, two AVITs are made for that issue.
    - AVIT that refers to the third-party vulnerability
    - AVIT that refers to the particular CVE
- If the Snyk issue is fixed on the Snyk side, only the AVIT that refers to the CVE will be closed, while the other AVIT will remain open.
- To avoid this case, follow the steps below to close AVIT manually.
    - Navigate to the Application Vulnerable Item "Application Vulnerability Response." Under it, click "Vulnerable Items" and then select "All."
    - Filter as "Source" "is" "Snyk," and then click on "Run" to view all the issues that are fetched from the Snyk.
    - Click the AVIT record that you want to close manually.
    - Click on the "Close" UI action.



7.3.3. The state of existing AVIT will not update from "Deferred" to Open when Triaging in ServiceNow is selected.

- An AVIT already fetched with Triaging in ServiceNow as false in vulnerability filtering will have a "Deferred" state if ignore is true. When Triaging in ServiceNow is selected, and integration is executed again, the existing AVIT state won't be updated to Open, as ServiceNow doesn't allow changing the state automatically if it is deferred.
- If you want to change the state from "Deferred" to "Open," you must do so manually. ServiceNow doesn't override the "Deferred" state to "Open."

7.3.4. Recently Ignored issues on the Snyk side could take ~5 hours to reflect in SCA V1 API.

- When the user ignores the issue from ServiceNow or manually ignores the SCA or IaC issue, it could take up to ~5 hours to reflect in GET v1 API.

7.3.5. Additional comments and state updates on the Snyk side may take up to ~9 hours in the US region. Typical performance is right away.

- When a user marks an AVIT as "Mark as False positive" or "Request Exception," then the "Additional comment" added by the user and the state of the issue will be updated to the Snyk platform after 9 hours (Ref).
- While changing the state of vulnerability from ServiceNow to Snyk, wait at least 9 hours to compare the state on Snyk with ServiceNow.

7.3.6. Users must be added to the approver group for performing "Mark as False positive" and "Request Exception."

- When the user marks an AVIT as "Mark as False Positive" or "Request Exception," the AVIT state will be set to "In Review," and the request must be approved.

- For users to approve the request of "Mark as False Positive," they must be in the "False Positive Approver" group.
- Users must be in the Application Exception Approver-Level 1 group to approve the request of "Request Exception."
- If users are not added to the group, the Request will be automatically rejected, as per ServiceNow VR default behavior.

- To avoid this case, ensure users are added to the approver group for performing "Mark as False positive" and "Request Exception."

7.3.7. Users must initiate the Reapply calculator's UI action inside the VR scope.

- If the user wants to change or reapply the Snyk calculator, ensure this is done in the Vulnerability Response scope.

7.3.8. Unable to "Mark as False positive" or "Request Exception" for IaC issues.

- If the user has set the REST mechanism for fetching the IaC issues in Global Settings and fetched IaC issues from integration, the integration cannot set an ignore on the Snyk platform.
- Release 3.0.0 version does not support the "Mark as false positive" or "Request exception" for IaC issues fetched from REST integration.

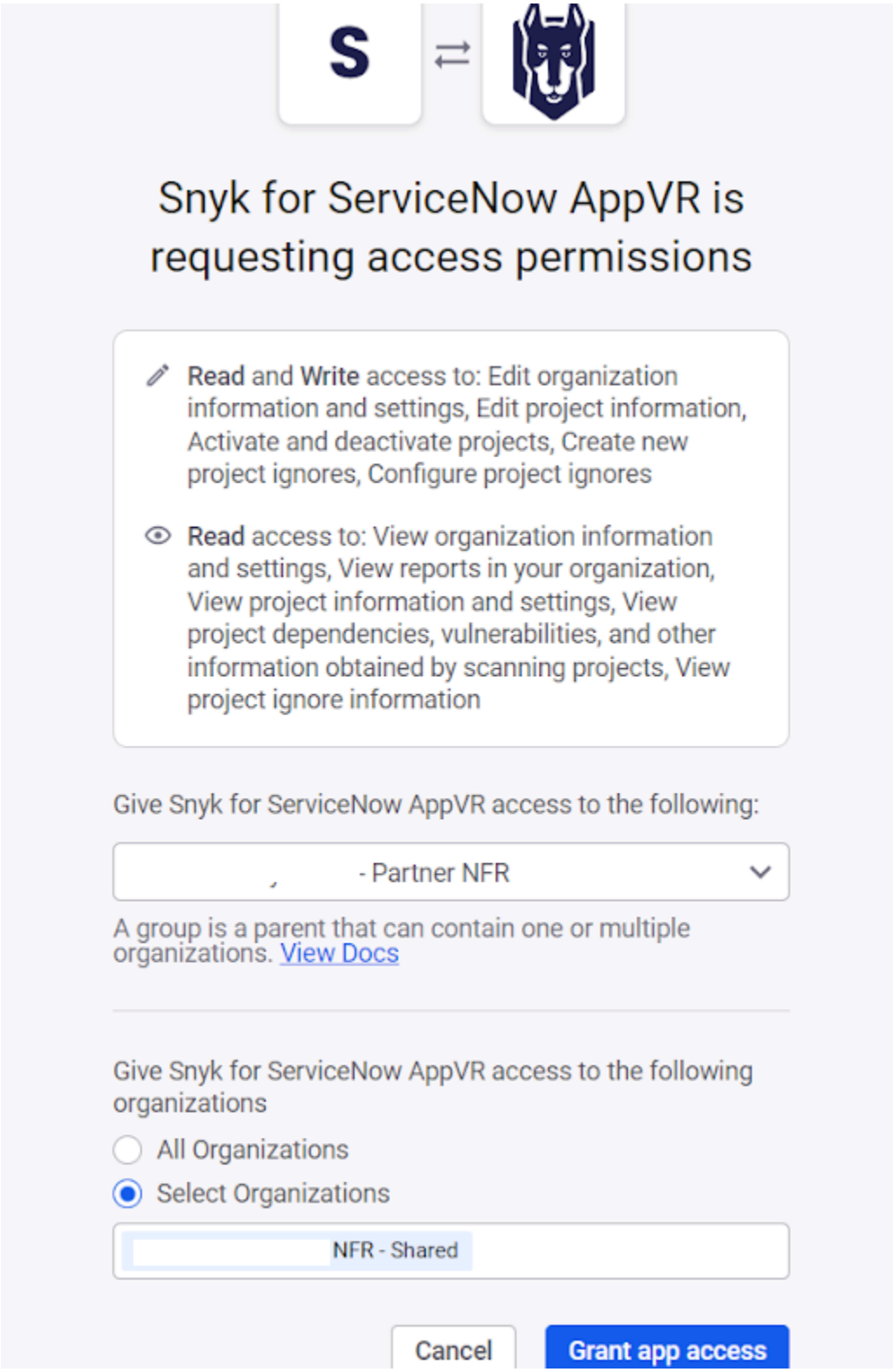
7.3.9. Use of "Move Project" V1 Snyk API can lead to unexpected results in SN Integration.

- Using the Snyk V1 "Move Projects" API to move a project will result in unexpected results, including the likelihood that the AVITs associated with the project will become orphaned in ServiceNow. The recommended process is to delete the target in Snyk and re-import the project into the new Org.

7.3.10. OAuth Process

- Snyk now allows customers to have a "Tenant" with multiple Groups. Customers may only select orgs from a single group during the OAuth process. A single integration will not import data across multiple groups due to the permission boundaries of the OAuth tokens.

The OAuth token process can only grant authorization to a SINGLE Org or all Orgs. Selecting multiple Orgs is currently unavailable and will be included in a future release.



END OF DOCUMENT…