Nexpose Ticketing System Integration Guide for ServiceNow

Contents

Last Revised: January 26, 17

Solution Summary

The goal of incident management is to restore normal service operation as quickly as possible following an incident, while minimizing impact to business operations and ensuring quality is maintained. The integration with Nexpose allows customers to create incident tickets based on vulnerabilities found across their systems. With this information in the ServiceNow platform, said tickets can be assigned to work teams, prioritized and resolved.

The ServiceNow Ticket Service integration creates reports based upon a scan of user selected sites or tags, depending on the configuration, and then creates tickets either for each machine and / or vulnerability, depending on the ticketing mode selected. On subsequent scans, the existing tickets are updated (and potentially closed) and new tickets are created, based on the delta from the previous scan.

This service can operate in Default, Vulnerability and IP mode. Tickets are not updated in Default mode.

The helper prepares tickets for sending to ServiceNow, formatting them depending on the selected ticketing mode. It is then responsible for sending new tickets, updating existing tickets and closing the correct tickets from the ServiceNow instance.

Installation and Configuration

Please see the Nexpose Ticketing Configuration Guide for how to install and configure the nexpose_ticketing Gem.

Once all dependencies have been installed, the configuration files need to be edited with the details of the target Nexpose and ServiceNow clients. To configure, open the configuration files under the config folder found in the Gem installation:

- Windows: C:\Ruby<version>\lib\ruby\gems\<version>\gems\nexpose_ticketing\lib\nexpose_ticketing\config
- Linux: /var/lib/gems/<version>/gems/nexpose_ticketing/lib/nexpose_ticketing/config

Your installation folder may differ; please refer to the Ruby documentation for the specific location.

The sites or tags which are to have tickets generated, as well as the ticketing mode, are defined in ticket_service.config. An example setup of this file can be found in the main Nexpose Ticketing Configuration Guide.

The JSON Web Service Module needs to be activated within ServiceNow before deployment of the Integration script. As of November 2013, the following steps are required to activate it:

1. Log into your ServiceNow instance using administrator credentials.
2. Navigate to System Definition > System Plugins.
   ~ Right-click the JSON plugin name on the list and select Activate/Upgrade
3. Click Activate
4. Create the transform maps and data using the ServiceNow Update set included in the gem under **lib/nexpose_ticketing/config/servicenow_updateset/**
5. Refer to the below documentation for information regarding Update Sets and the ServiceNow installation.

ServiceNow documentation on using and creating UpdateSets:

http://wiki.servicenow.com/index.php?title=Getting_Started_with_Update_Sets

http://wiki.servicenow.com/index.php?title=Using_Update_Sets#gsc.tab=0

http://wiki.servicenow.com/index.php?title=Saving_Customizations_in_a_Single_XML_File#gsc.tab=0

The log-in details are specified within the servicenow.config file. Open the file using any text editor and note the following options:

Setting	Description	Sample Value
product	Name of the ticketing service.	ServiceNow*
vendor	Name of the ticketing software developer.	ServiceNow*
helper_name	This is the helper class name. This should not be changed.	ServiceNowHelper*
servicenow_url	URL to the ServiceNow incident creation JSON page. This will usually have ?JSON at the end of the URL.	http://my.service-now.com/incident.do?JSON
username	Username of a user within ServiceNow with rights to create, update, and close incidents.	servicenowuser
password	Password of above username	password
verpose_mode	Determines if SSL connections will output to stderr	N
redirect_limit	Should the above URL result in a 301/302 redirect, the redirect_limit determines how many times the service should follow the redirect before ending execution with an error.	10

* These values should not be changed.

Initial Run

Assuming you've properly configured the Nexpose and ServiceNow parameters, execute the following command within the 'bin' folder to run the service:

- ruby nexpose_ticketing servicenow

Every time this command is executed, the service will query Nexpose and obtain any new vulnerability information and open tickets accordingly.

To view log information, wait for the service to complete execution and then review the logs located in the **/lib/nexpose_ticketing/log** directory**.**

As part of a continuous ticketing program, it is recommended to run the command daily via a Cron job or Windows task.

Troubleshooting

The most common errors when running the script are:

- Configuration errors (such as incorrect indentation or user details).
- Specifying a Nexpose user without permission to create reports.
- Not specifying a site or tag.
- Specifying both a tag and a site. The tag will take priority and the site will not be scanned.

If not enabled, enable logging and view the log files after re-running the service. These files will contain any error information and will also contain information statements about what vulnerability data was found in Nexpose and transmitted to ServiceNow.

If everything still fails, please send an email to support@rapid7.com with the ticket_helper.log and ticket_service.log attached and a description of the issue.

Helper Method Overview

There are several methods implemented in the serviceNow_Helper common to all helpers, for creating, updating and closing tickets, as well as several ServiceNow specific methods. Below is an outline of the methods, along with an explanation of when they are called and how they work:

create_tickets

- Description: This method is used to send new tickets to the ServiceNow instance. An array of prepared tickets to create is provided to the method. It then calls the submit_ticket method for each ticket in the array.
- Used By: This method is called from the all_site_report, full_site_report and delta_site_new_scan methods in ticket_service.rb to send new tickets to the ServiceNow service after they have been discovered and prepared.

update_tickets

- Description: This method is used to send tickets to the ServiceNow instance on subsequent runs, after the initial tickets have been created in IP and Vulnerability mode. It takes an array of tickets as the parameter and calls the submit_ticket method for each ticket in the array.
- Used By: This method is called from the delta_site_new_scan method in ticket_service.rb when in IP and vulnerability mode to update existing tickets in ServiceNow

close_tickets

- Description: This method is used to send a list of prepared ticket closure messages to the ServiceNow instance. It takes an array of tickets as the parameter and calls the submit_ticket method for each ticket in the array.
- Used By: This method is called from the delta_site_new_scan method in ticket_service.rb to close existing tickets. It is used in all 3 ticket generation modes.

send_ticket

- Description: This method is used to post an individual JSON formatted ticket to ServiceNow. This method takes the ticket to send, the URL to send the ticket to and the retry limit for the ticket. It creates a new HTTP POST request and appends the authorisation for the ServiceNow instance and the ticket, before sending it. If the response from the post is a 301/302 redirect, the method will attempt to resend the ticket to the response's location for up to [limit] times (which starts at the redirect_limit config value and is decremented with each redirect response.)
- Used By: This method is called by create_tickets, update_tickets and close_tickets to send prepared tickets to ServiceNow.

prepare_create_tickets

- Description: This method is called to choose the correct 'matching fields' for the current ticketing mode before calling the prepare tickets method. This value is used to group related vulnerability information together when creating tickets. The matching fields value is chosen based upon the current ticketing mode and how the information is to be grouped per ticket: Individual vulnerability to IP for Default mode; by Individual IP for IP mode; and by Vulnerability for Vulnerability mode. After choosing the correct matching field, the method calls prepare_tickets to correctly format the tickets for sending.
- Used By: This method is called from the all_site_report, full_site_report and delta_site_new_scan methods in ticket_service.rb to prepare and format new tickets for sending to the ServiceNow instance.

prepare_tickets

- Description: This method is called to prepare a list of vulnerabilities, converting them into JSON format for sending to the ServiceNow instance. Using the matching fields variable, this method groups related rows from the CSV file together into a single ticket. For each row corresponding to a new ticket in the CSV file, a new ticket object will be created with the correct values. If this ticket is for a newly discovered vulnerability or asset with a vulnerability, the ticket is given the action of 'Insert', for existing tickets it is set to 'Update'. For every subsequent row that is part of the same ticket, the ticket description will be updated by the common_helper.rb class. When a new group of rows is encountered, the current object is converted into JSON and appended to the array of ticket objects. The row is then used as the basis for the next ticket. This array of tickets is the returned to the parent method.
- Used By: This method is called from the prepare_create_tickets and the prepare_update_tickets methods to prepare a list of vulnerabilities into formatted tickets for sending to ServiceNow.

prepare_update_tickets

- Description: This method is called to choose the correct 'matching fields' for the current ticketing mode when doing an update before calling the prepare tickets method. This value is used to group related vulnerability information together when creating tickets. The matching fields value is chosen based upon the current ticketing mode and how the information is to be grouped per ticket: by Individual IP for IP mode; and by Vulnerability for

Vulnerability mode. After choosing the correct matching field, the method calls prepare_tickets to correctly format the tickets for sending. The list of vulnerabilities are ordered depending on the ticketing mode and then by ticket_status, allowing the method to loop through and display new, old, and same vulnerabilities / assets, in that order.

- Used By: This method is called from the delta_site_new_scan method in ticket_service.rb when in IP and vulnerability mode.

prepare_close_tickets

- Description: This method is used to prepare a list of ticket closures from the CSV of vulnerabilities exported from Nexpose to send to the ServiceNow instance. For each ticket in the CSV, the method first generates the NXID. It then creates a JSON object with an action of update, a query containing the NXID and the state set to the closure value in ServiceNow. This ticket is then appended to an array of ticket closures to be sent to serviceNow.
- Used By: This method is called from the delta_site_new_scan method in ticket_service.rb to create ticket closure messages for sending to ServiceNow. This is used in all three ticketing modes.