Integration Guide

ServiceNow <-> Nexpose Integration

Vulnerability -> Ticket workflow

Partner Name:	ServiceNow
Website:	http://www.servicenow.com
Product Name:	ServiceNow Incident
Version:	Darwin
Import Type:	Automated via API

Last Revised: November 10, 2013

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, update, and close ticket incidents based on vulnerabilities found across their systems. With this information in their ServiceNow platform, said tickets can be assigned to work teams, prioritized and resolved.

Partner Product Configuration

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:

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

As always, check ServiceNow documentation for further information.

Introduction

This document will guide you through all the steps necessary to configure the Nexpose ticketing service to successfully import, update, and close Nexpose vulnerability data transmitted to the ServiceNow incident ticketing system.

Installation

ServiceNow integration with Nexpose requires nexpose_ticketing, a Ruby gem that facilitates communication between Nexpose and various ticketing services.

Before installing the nexpose_ticketing gem, a Ruby interpreter must be installed on the system running the gem. The following link shows the different options for installing Ruby in several platforms:

https://www.ruby-lang.org/en/downloads/

RubyGems is the other pre-installation requirement for using nexpose_ticketing. After successfully installing a Ruby interpreter, install RubyGems. The following link shows the different options for installing RubyGems in several platforms:

http://rubygems.org/

After installing Ruby and RubyGems, install nexpose_ticketing by opening a command prompt or terminal window with Ruby and RubyGems added to the PATH and run the following command:

```
gem install nexpose_ticketing
```

This command will install the ticketing gem and all necessary prerequisites.

Configuration

Configuring ServiceNow integration with Nexpose requires modifying two config files from within the gem. First, locate the directory of the installed nexpose_ticketing gem. This varies from system to system. Once located, all configuration files are in the /lib/nexpose_ticketing/config directory.

ticket_service.config

Open ticket_service.config using any text editor and note the following configuration options:

Setting	Description	Sample Value
logging_enabled	Specifies if the ticketing service logs information to a text file. Log files are saved in the /log directory.	true
sites	Determines if Nexpose reports on vulnerabilities for one or more site IDs. Leave blank to	- '1' - '4'
severity	Minimum floor severity to report vulnerabilities to the ticket service.	8
ticket_mode	Determines how tickets are generated in the target ticket service. Two options are currently available: - 'I' creates one ticket per IP address with all vulnerabilities found for the IP address - 'D' creates one ticket per vulnerability	D
nxconsole	Host name of the Nexpose server	127.0.0.1
nxuser	Username of a user within Nexpose with report generation rights.	nxadmin
nxpasswd	Password of above username	password

Note that all options are case-sensitive.

servicenow.config

Open servicenow.config using any text editor and note the following configuration options:

Setting	Description	Sample Value
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
verbose_mode	Determines if SSL connections will output to	N

	stderr.	
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

Execution

To run the ServiceNow integration, open a command prompt or terminal window with Ruby and RubyGems added to the PATH and run the following command:

```
nexpose_servicenow
```

The service will run as a foreground task and end after completing execution. In a successful run of the service, there should be no output to the command prompt or terminal window.

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

To further automate execution of the ServiceNow integration, consider running the integration as a cron job.

Troubleshooting

The most common errors when running the script are configuration based, users without permission to create tickets or generate reports with Nexpose, incorrect passwords or not specifying a site or asset group when configuring the script.

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 integrations_support@rapid7.com with the ticket_helper.log and ticket_service.log attached and a description of the issue.