Integration Guide

Remedy <-> Nexpose Integration

Vulnerability -> Ticket workflow

Partner Name: Remedy

Website: http://www.bmc.com/it-solutions/remedy-itsm.html

Product Name: BMC Remedy ITSM

Version: 8.1

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 Remedy platform, said tickets can be assigned to work teams, prioritized and resolved.

Partner Product Configuration

There is no additional configuration required to use the Nexpose ticketing service with Remedy.

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 Remedy ITSM.

Installation

Remedy 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

Prior to setting up the necessary configuration, it is important to understand how communication with Remedy occurs. Remedy exposes SOAP web services for systems such as nexpose_ticketing to consume. However, in a default installation of Remedy, the web services' WSDLs are secured in such a way that accessing them remotely is not possible. While you can enable this access, Rapid7 wishes to reduce end-user configuration as much as possible and with that in mind, local copies of the incident creation WSDLs are installed as part of the nexpose_ticketing installation process. This means that under most common scenarios the only web service configuration required is setting up the proper web service endpoints.

Configuring Remedy ITSM 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.

remedy.config

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

Setting	Description	Sample Value
create_soap_endpoint	URL to the Remedy creation SOAP Interface endpoint.	http://url/arsys/services/ARService?server=bmc-remedy-w&webService=HPD_IncidentInterface_Create_WS
query_modify_soap_endpoint	URL to the Remedy modification SOAP interface endpoint	http://url/arsys/services/ARService?server=bmc-remedy-w&webService=HPD_IncidentInterface_WS
username	Username of a user within Remedy with rights to create, update, and close incidents.	username
password	Password of above username	password
authentication	If the Remedy instance uses authentication codes in combination with username/password, then specify it here. Authentication code is not required.	mysecretcode

first_name	First name of the above username. Remedy requires you include this data with web service requests.	John
last_name	Last name of the above username. Remedy requires you include this data with web service requests.	Doe
open_timeout	Timeout (in seconds) for opening a SOAP connection.	30
read_timeout	Timeout (in seconds) for reading a SOAP response.	30

Note: Finding Web Service Endpoints

In many cases, the sample endpoints above (substituting the actual URL for http://url) will work with no issue. However, here are the steps to verify the endpoints are correct:

1. Navigate to the list of web services on the Remedy instance at https://<midtierServer>/arsys/WSDL/protected/list
2. Click on the HPD_IncidentInterface_Create_WS link
3. Scroll to the bottom of the XML document and note the XML node <soap:address… />
4. Copy the location attribute for create_soap_endpoint

Replicate the above steps, substituting HPD_IncidentInterface_WS for the web service link and query_modify_soap_endpoint for the location attribute.

Execution

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

```
nexpose_remedy
```

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 Remedy 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 Remedy.

Some additional troubleshooting notes:

- Many Remedy installation are on non-standard ports (80 and 443). Web service connectivity could run into issues if you do not specify the correct port in the two endpoints.
- If the web services connect successfully but cannot create incidents, there may be an issue with automatic assignment of incidents. In the current version of Nexpose-to-Remedy integration, automatic group assignment of incidents must be enabled or incident creation will fail. Configure group assignment using the Application Administration Console from within Remedy.
- Newer versions of Remedy may have slightly updated WSLDs. In the case that the WSDL on the Remedy instance differs from the one located in /lib/nexpose_ticketing/config/remedy_wsdl, please contact Rapid7 for assistance.

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.