RAPID7 Nexpose Integration Guide for JIRA

Ticketing Solution

Partner Name: JIRA

Website: https://www.atlassian.com

Product Name: JIRA

Version: 6

Import Type: Automated via API

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

Partner Product Configuration

Under the JIRA Product, a valid username/password should be created and a project key setup. All tickets opened will be under the "Task" type.

Introduction

This document will guide you through all the steps necessary to configure the JIRA Implementation to successfully import Nexpose vulnerability data into the JIRA ticketing system.

Before you begin

The integration was created using Ruby, as such, a Ruby interpreter must be installed on the system where it's going to run. The following link shows the different options for installing Ruby in several platforms:

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

Please install the codebase that best suits your environment.

Once installed, the following Ruby Gem must be installed:

> nexpose_ticketing : This installation can usually be performed by issuing the command 'gem install nexpose_ticketing' from the command line / bash.

On some systems, dependencies might need to be installed prior to the installation of each Gem. Please refer to their appropriate documentation for instructions.

Configuring the script

Once all dependencies have been installed, the implementation should now be configured. 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.

Rapid7 Corporate Headquarters   800 Boylston Street, Prudential Tower, 29th Floor, Boston, MA 02199-8095   617.247.1717   www.rapid7.com

2

There should be two files present in the config folder: ticket_service.config, jira.config

Please make sure you've provided the appropriate values in ticket_service.config:

> **nxconsole**: {IP ADDRESS OF NEXPOSE CONSOLE}

> **nxadmin**: {USER ID WITH SUFFICIENT PRIVILEGES}

> **nxadmin**: {PASSWORD}

> **ticket_mode**: {ticket creation preference, see below}

Note: There are two modes for ticket creation, please choose whichever best suites your needs:

❖ **D** -- Creates one ticket per IP *per* vulnerability. This may have the potential to create numerous tasks within Jira

❖ **I** -- Creates one ticket per IP and rolls all the vulnerabilities into the single task.
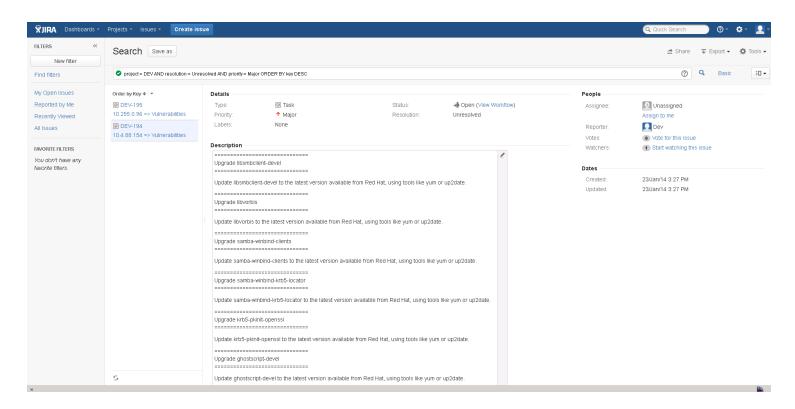
Populate the following values in the jira.config:

> **helper_name:** JiraHelper => **Leave as is**

> **username:** {USERNAME OF JIRA USER}

> **password:** {JIRA PASSWORD}

> **project: ProjectKey**

Running for the first time

Assuming you've properly configured the Nexpose and JIRA parameters, issue the command "**nexpose_jira**" from a command/bash shell. Every time this command is run the service will query Nexpose and obtain any new vulnerability information and open tickets accordingly.

As part of a continuous ticketing program, setup the command to be run under a cron job or windows task at least once a day.

Rapid7 Corporate Headquarters   800 Boylston Street, Prudential Tower, 29th Floor, Boston, MA 02199-8095   617.247.1717   www.rapid7.com

3

What if something goes wrong?

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.

We recommend reading the log file under the log folder in the Gem.

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

Rapid7 Corporate Headquarters   800 Boylston Street, Prudential Tower, 29th Floor, Boston, MA 02199-8095   617.247.1717   www.rapid7.com

4