How-To Guide

Tenable.io for Red Hat Satellite

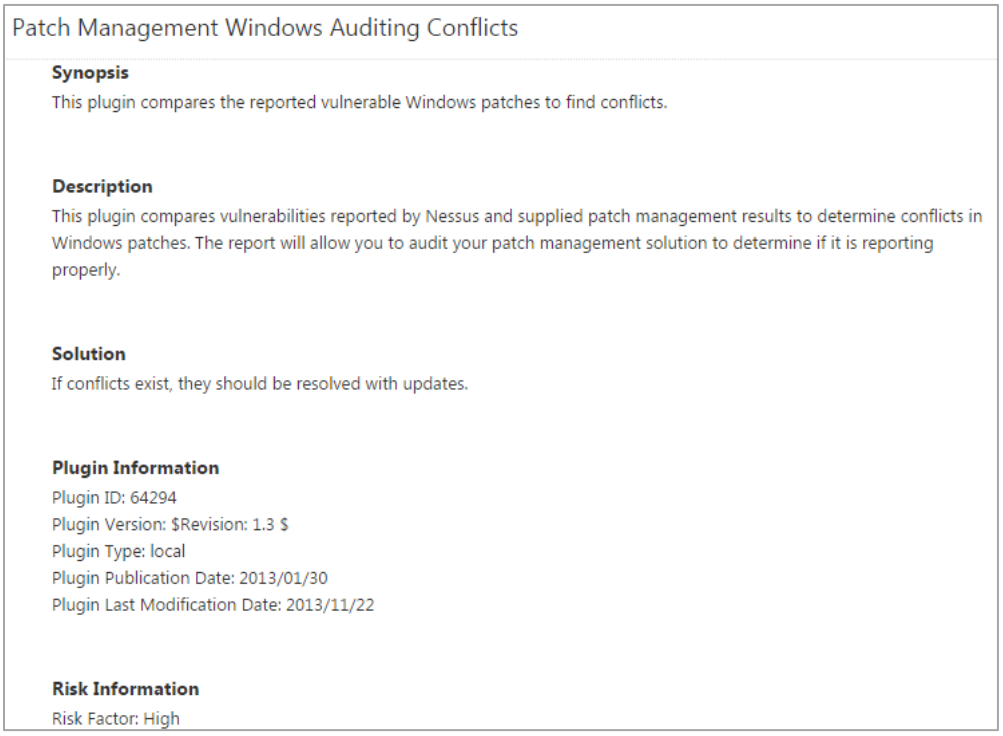
Introduction

Tenable provides a broad spectrum of coverage and integration support, including active scanning, passive monitoring, intelligent connectors, agent scanning and host activity data collection. Tenable patch management integrations identify hosts that have fallen out of management or are not functioning properly, identifying hosts missing patches so you can fix them.

Tenable.io™ leverages credentials for the Red Hat Satellite patch management system to perform patch auditing on systems for which credentials may not be available to Tenable.io.

IT administrators are expected to directly manage the patch monitoring software and install any agents required by the patch management system on their systems.

If credentials are provided for a host, as well as a patch management system or multiple patch management systems, Tenable.io will compare the findings between all methods and report on conflicts or provide a "satisfied" finding. For example, if you provide credentials for the target host and multiple patch management systems, Tenable.io will produce a report with a "High" severity rating, if there are conflicts found:


Patch Management Windows Auditing Conflicts

Synopsis

This plugin compares the reported vulnerable Windows patches to find conflicts.

Description

This plugin compares vulnerabilities reported by Nessus and supplied patch management results to determine conflicts in Windows patches. The report will allow you to audit your patch management solution to determine if it is reporting properly.

Solution

If conflicts exist, they should be resolved with updates.

Plugin Information

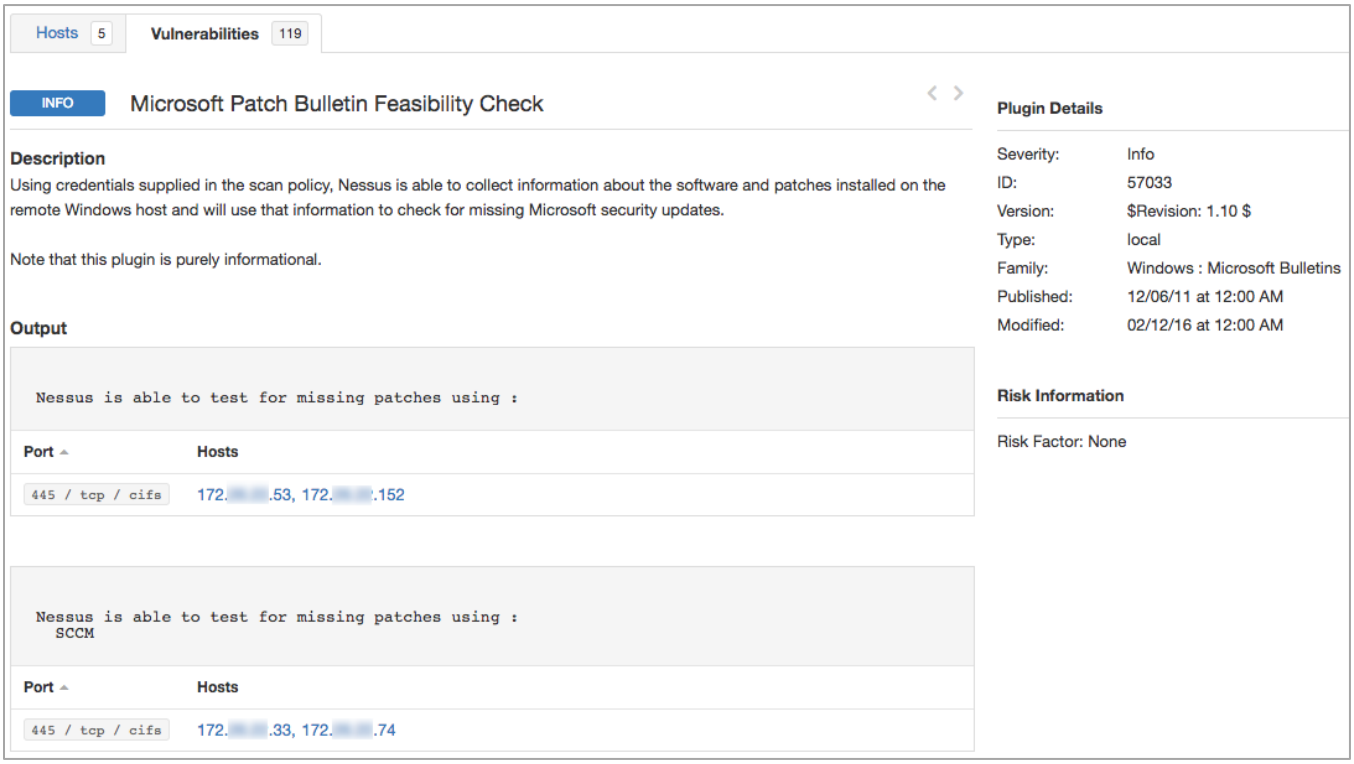
Plugin ID: 64294
Plugin Version: $Revision: 1.3 $
Plugin Type: local
Plugin Publication Date: 2013/01/30
Plugin Last Modification Date: 2013/11/22

Risk Information

Risk Factor: High

This underscores the importance of cross-referencing patches between what is on the system and what the patch management system thinks is on the system. The report for each patch and the discrepancies is displayed in the plugin output. Conflicts indicate that the affected host was not targeted for deployment of a particular patch, so the patch management system does not detect it as missing.

This allows organizations to not only audit hosts, but to help ensure that patch management software is configured properly and providing accurate information. If there are no conflicts found, Tenable.io will provide a “Satisfied” finding with an “Info” severity rating:



Red Hat Satellite

Red Hat Satellite is a systems management platform for Linux-based systems. Tenable.io has the ability to query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information through the Tenable.io UI.

Although not supported by Tenable, the Red Hat Satellite plugin will also work with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk has the capability of managing distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

- If a credentialed check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Tenable.io is able to connect to the target system, it will perform checks on that system and ignore Red Hat Satellite output.
- The data returned to Tenable.io by Red Hat Satellite is only as current as the most recent data that the Satellite server has obtained from its managed hosts.

Satellite scanning is performed using five Tenable.io plugins:

- Patch Management: Patch Schedule From Red Hat Satellite Server (Plugin ID 84236)
- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 84235)
- Patch Management: Red Hat Satellite Server Get Managed Servers (Plugin ID 84234)
- Patch Management: Red Hat Satellite Server Get System Information (Plugin ID 84237)
- Patch Management: Red Hat Satellite Server Settings (Plugin ID 84238)

If the Red Hat Satellite server is version 6, three additional Tenable.io plugins are used:

- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 84231)
- Patch Management: Red Hat Satellite 6 Settings (Plugin ID 84232)
- Patch Management: Red Hat satellite 6 Report (Plugin ID 84233)

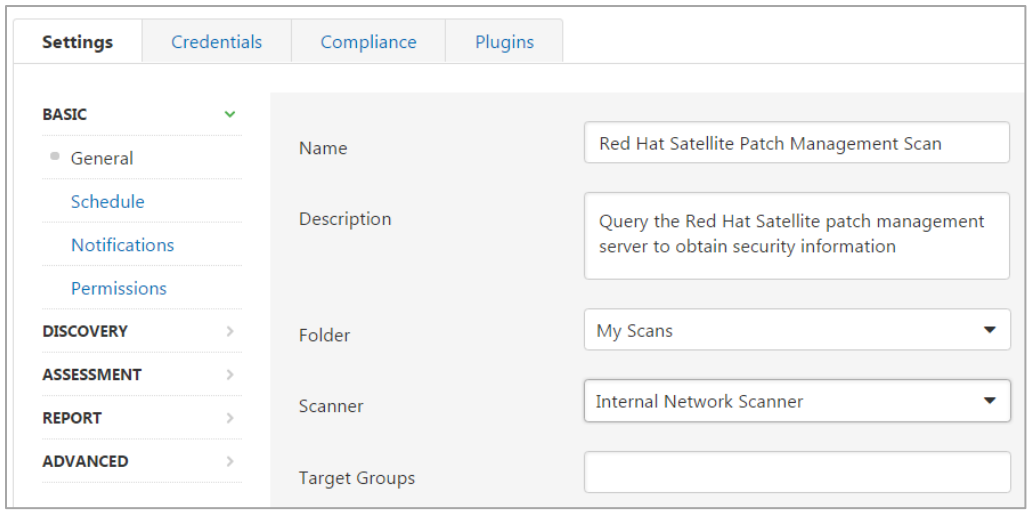
Creating the Policies

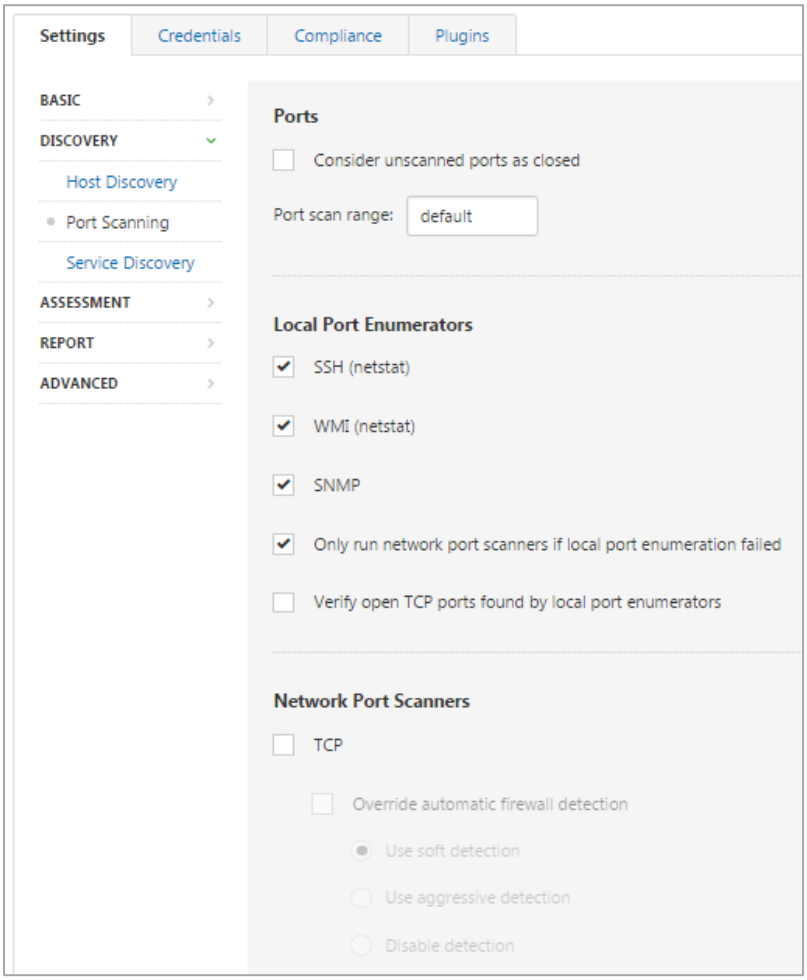
From the Tenable.io web interface, click the "**Scan**" tab and then "**New Scan**." Select the "**Advanced Network Scan**" template.

Directions for each tab under the "**General**" menu are described in this section.

General Settings

If Red Hat Satellite patch management scans are run as part of a normal scan, all port scanning settings can be configured as they would in a typical scan policy.

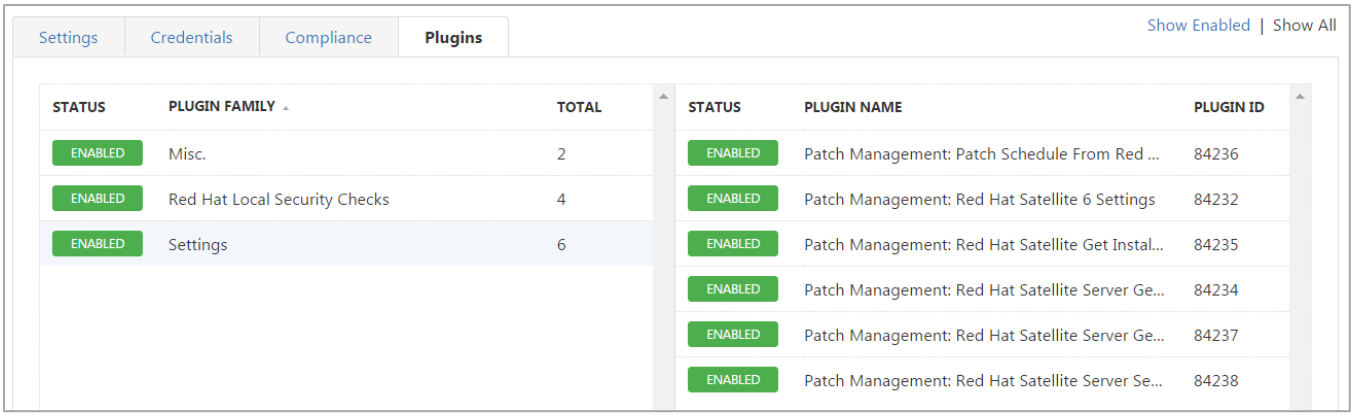




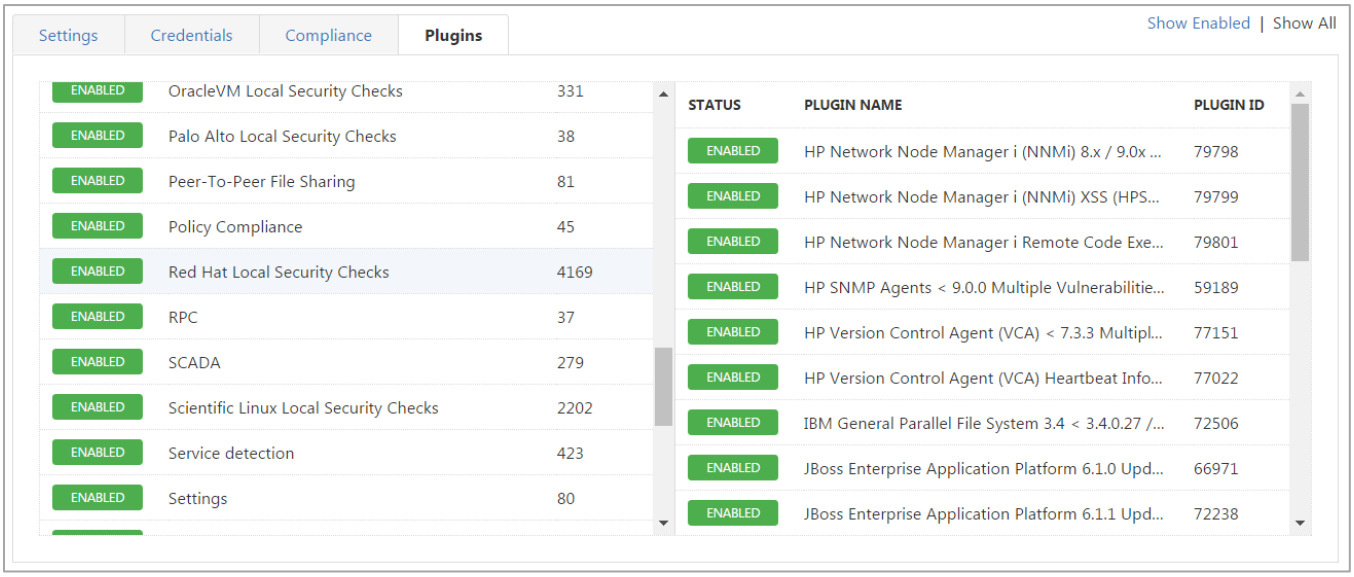
For more information on the options under "**Settings**," see the Tenable.io User Guide.

Plugins

At least five specific plugins must be enabled for the Satellite patch management scans to run (see above for full list). These plugins can easily be found by searching for "Red Hat Satellite" through the "Plugin Name" advanced filter:

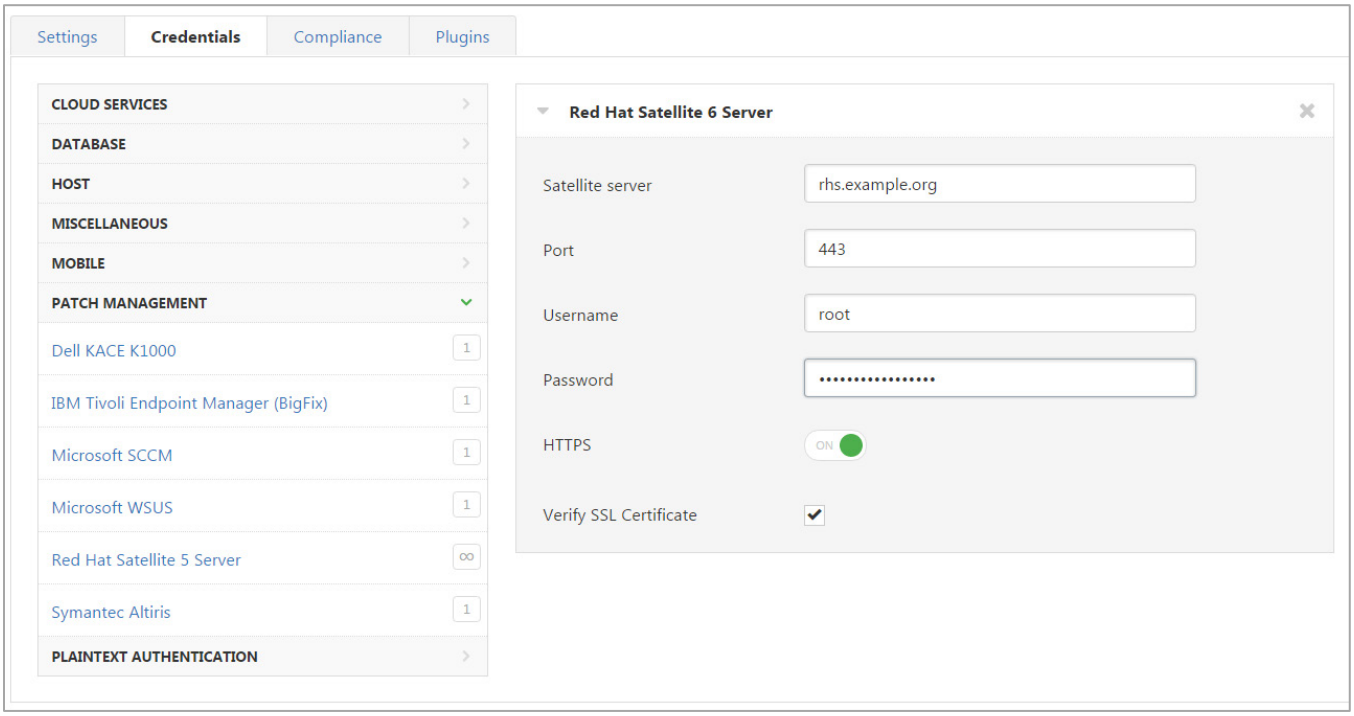


In addition, enable the local operating system security check plugins of your choice. Tenable.io currently supports Red Hat Enterprise Server, Fedora, openSUSE and CentOS in conjunction with the Red Hat Satellite Server plugins:



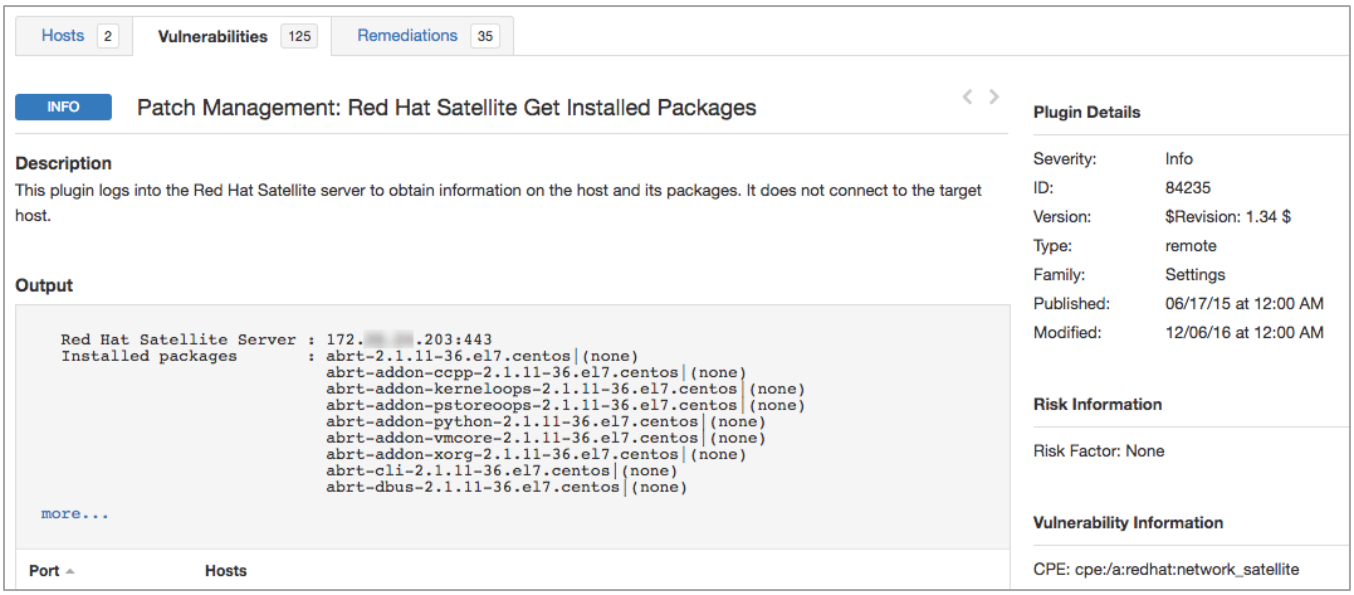
Preferences

Credentials for the Red Hat Satellite system must be provided for Satellite scanning to work properly. Under the "**Credentials**" tab in Tenable.io, select "**Patch Management**" and then "**Red Hat Satellite 5 Server**" or "**Red Hat Satellite 6 Server**":

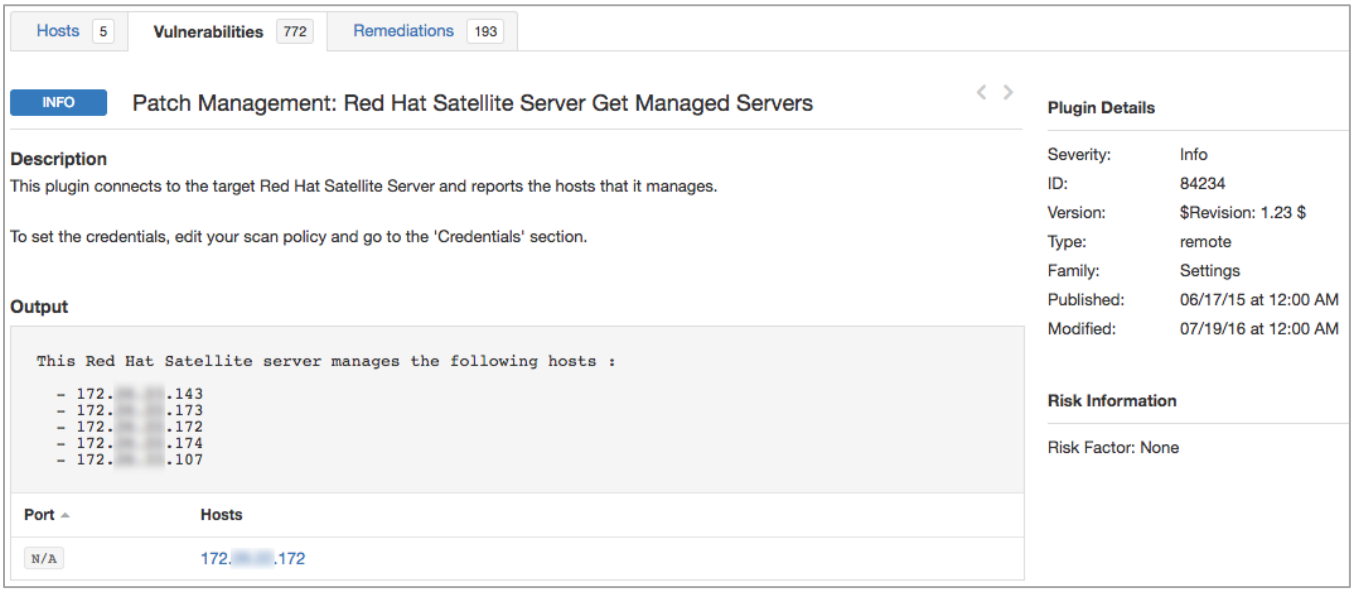


Credential	Description
Red Hat Satellite server(s)	Red Hat Satellite IP address or system name
Red Hat Satellite port(s)	Port Satellite is running on (Typically TCP 80 or 443)
Red Hat Satellite username(s)	Satellite username
Red Hat Satellite password(s)	Satellite password

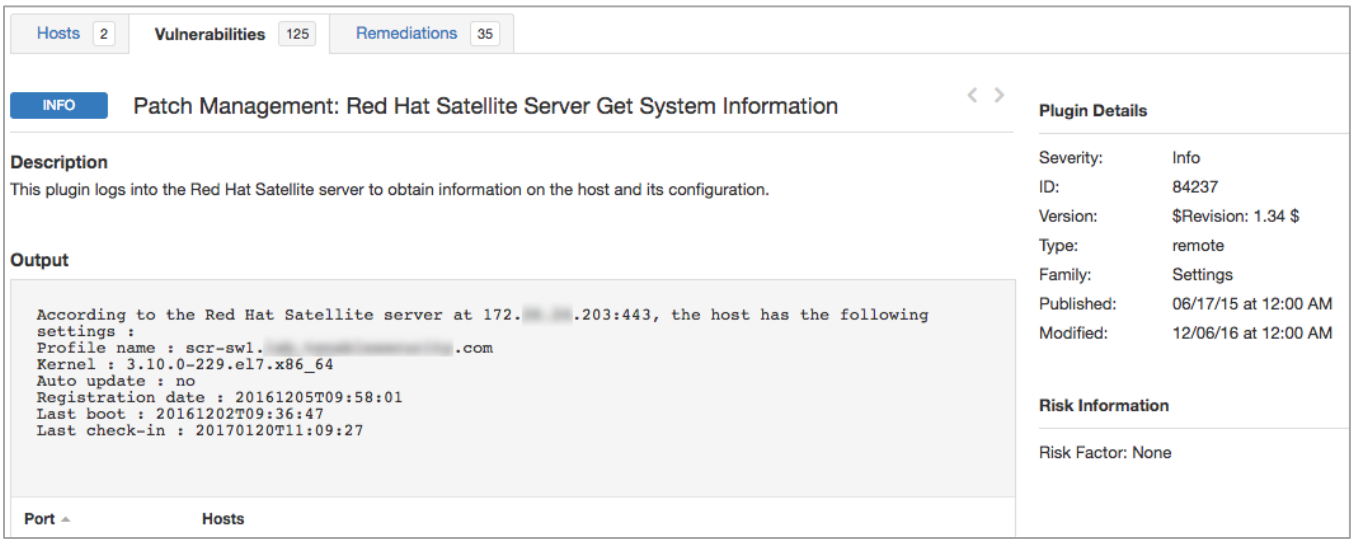
When reporting system findings, Tenable.io will report from Red Hat Satellite the list of installed packages on the host:



Tenable.io will also report from Red Hat Satellite the list of managed hosts:



Additionally, Tenable.io will report from Red Hat Satellite's findings on a managed host's configuration:



About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.