Patch Management Integration

January 10, 2012

(Revision 5)
# Table of Contents

## Overview

Scanning With Multiple Patch Managers ................................................................. 3

## WSUS

Creating the Policies ................................................................................................. 3

- General ............................................................................................................... 4

- Credentials ........................................................................................................ 4

- Plugins ............................................................................................................... 4

- Preferences ....................................................................................................... 5

## SCCM

Creating the Policies ................................................................................................. 8

- General ............................................................................................................... 8

- Credentials ........................................................................................................ 9

- Plugins ............................................................................................................... 9

- Preferences ....................................................................................................... 10

## VMware Go

Creating the Policies ............................................................................................... 11

- General ............................................................................................................. 11

- Credentials ...................................................................................................... 12

- Plugins ............................................................................................................. 12

- Preferences ...................................................................................................... 13

## Red Hat Network Satellite

Creating the Policies ............................................................................................... 15

- General ............................................................................................................. 15

- Credentials ...................................................................................................... 16

- Plugins ............................................................................................................. 16

- Preferences ...................................................................................................... 17

## About Tenable Network Security

................................................................................................................................. 20
OVERVIEW
Tenable’s Unified Security Monitoring (USM) product suite provides great flexibility in scanning methods to better serve our customers’ varying scanning requirements and restrictions. Customers can perform passive scanning, active network scans, or scan with credentials for more accurate results with less network bandwidth utilization.

Nessus and SecurityCenter now leverage credentials for the WSUS, SCCM, and VMware Go (formerly Shavlik) patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner.

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

SCANNING WITH MULTIPLE PATCH MANAGERS
If multiple sets of credentials are supplied to Nessus for patch management tools, Nessus will not use all of them. Based on the credentials supplied, Nessus will use the first one available in the following order:

1. Credentials supplied to directly authenticate to the target
2. VMware Go (formerly Shavlik)
3. WSUS
4. SCCM

WSUS
Windows Server Update Services (WSUS) is available from Microsoft to manage the distribution of updates and hotfixes for Microsoft products. Nessus and SecurityCenter have the ability to query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Nessus or SecurityCenter GUI.

If the credential 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 Nessus is able to connect to the target system, it will perform checks on that system and ignore WSUS output.

The data returned to Nessus by WSUS is only as current as the most recent data that the WSUS server has obtained from its managed hosts.

WSUS scanning is performed using two Nessus plugins:

- wsus_init_info.nbin (Plugin ID 57031)
- wsus_get_missing_updates.nbin (Plugin ID 57032)

CREATING THE POLICIES
From the Nessus or SecurityCenter web interface, click the “Policies” tab and then “Add”. Directions for each tab under the “Add Policy” menu are described in this section.
General
If WSUS patch management scans are run as part of a normal scan or SMB scan, all port scanning settings can be configured as they would in a typical scan policy.

Credentials
Because Nessus does not rely on the system being managed by WSUS to report patch management issues, credentials for the target systems do not need to be used in the scan policy.

Plugins
At least three specific plugins must be enabled for the WSUS patch management scans to run. These plugins can easily be found by searching for “WSUS” or “Patch Management” on the plugin filtering configuration page:
Patch Management: WSUS Server Settings

Preferences
Credentials for the WSUS server must be provided for WSUS scanning to work properly.

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSUS Server</td>
<td>WSUS IP address or system name</td>
</tr>
<tr>
<td>WSUS Port</td>
<td>Port WSUS is running on (Typically TCP 80 or 443)</td>
</tr>
<tr>
<td>WSUS Username</td>
<td>WSUS admin username</td>
</tr>
<tr>
<td>WSUS Password</td>
<td>WSUS admin password</td>
</tr>
</tbody>
</table>

In the “Preferences” pane, select “Patch Management: WSUS Server Settings” from the Plugin drop-down menu:
Plugin Name: MS11-094: Vulnerability in Internet Information Services (IS) FTP Service Could Allow Remote Code Execution (2446256)

Synopsis: The FTP service running on the remote host has a memory corruption vulnerability.

Description:
The 433 FTP service running on the remote host has a heap buffer overflow vulnerability. The "TELNET_STREAM_CONTEXT-OrSentData" function fails to properly sanitize user input, resulting in a buffer overflow.

Solution:
An unauthenticated remote attacker can exploit this to execute arbitrary code.

Solution:
Microsoft has released a set of patches for Windows Vista, 2008, 2008 R2, and 7:

http://www.microsoft.com/technet/security/bulletin/1.064.mspx

CVSS Base Score:
10.0 (CVSS2:MAV/AV:N/AC:L/AV:N/AC:C/AU:N/C:C/I:C/A:C)

CVSS Temporal Score:
7.3 (CVSS2:MAV/AV:N/AC:L/AV:N/AC:C/AU:N/C:C/I:C/A:C)

Plugin Output:
The host is missing KB 2446256 according to WBUS.

CVE:
CVE-2010-3072

OS:
RHEL 4.5.0

Vulnerability Publication Date:
2010/12/21
SCCM
System Center Configuration Manager (SCCM) is available from Microsoft to manage large groups of Windows-based systems. Nessus has the ability to query SCCM to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the Nessus or SecurityCenter GUI.

> If the 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 Nessus is able to connect to the target system, it will perform checks on that system and ignore SCCM output.
> The data returned by SCCM is only as current as the most recent data that the SCCM server has obtained from its managed hosts.

SCCM scanning is performed using two Nessus plugins:

> sccm_init_info.nbin (Plugin ID 57029)
> sccm_get_missing_updates.nbin (Plugin ID 57030)

Creating the Policies
From the Nessus or SecurityCenter web interface, click the “Policies” tab and then “Add”. Directions for each tab under the “Add Policy” menu are described in this section.

General
If SCCM patch management scans are run as part of a normal scan or SMB scan, all port scanning settings can be configured as they would in a typical scan policy.
**Credentials**
Because Nessus scans do not rely on the system being managed by SCCM to report patch management issues, credentials for the target systems do not need to be used in the scan policy.

**Plugins**
At least three specific plugins must be enabled for the SCCM patch management scans to run. These plugins can easily be found by searching for “SCCM” or “Patch Management” on the plugin filtering configuration page:

![Patch Management: SCCM Server Settings](image1)

![Patch Management: Missing updates from SCCM](image2)
Preferences

Credentials for the SCCM server must be provided for SCCM scanning to work properly.

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCM Server</td>
<td>SCCM IP address or system name</td>
</tr>
<tr>
<td>SCCM Domain</td>
<td>The domain the SCCM server is a part of</td>
</tr>
<tr>
<td>SCCM Username</td>
<td>SCCM admin username</td>
</tr>
<tr>
<td>SCCM Password</td>
<td>SCCM admin password</td>
</tr>
</tbody>
</table>

In the “Preferences” pane, select “Patch Management: SCCM Server Settings” from the Plugin drop-down menu:
VMWARE GO

VMware Go (formerly known as Shavlik) is a cloud-based service that checks the patch compliance status of an organization’s systems. Nessus and SecurityCenter have the ability to query VMware Go to verify whether or not patches are installed on systems managed by VMware Go and display the patch information through the Nessus or SecurityCenter GUI.

- The VMware Go plugin never makes a direct connection to the target system; it instead connects to the VMware Go server specified to query the host about patch status.
- Outbound access to the VMware Go management server is required.
- SMB credentials are given priority; VMware Go is not used on a host when a valid SMB account is given.
- The organization using VMware Go is responsible for installing the VMware Go agents on their hosts.
- The data returned to Nessus by VMware Go is only as current as the most recent data that the VMware Go.

VMware Go scanning is performed using three Nessus plugins:

- shavlik_settings.nbin (Plugin ID: 57026)
- shavlik_host_info.nbin (Plugin ID 57027)
- shavlik_missing_patches.nbin (Plugin ID 57028)

CREATING THE POLICIES

From the Nessus or SecurityCenter web interface, click the “Policies” tab and then “Add”. Directions for each tab under the Add Policy menu are described in this section.

General

If VMware Go patch management scans are run as part of a normal scan or SMB scan, all port scanning settings can be configured as they would in a typical scan policy.
**Credentials**
Because VMware Go scans do not rely on the system being managed to report patch management issues, credentials for the systems do not need to be used in the scan policy.

**Plugins**
Make sure the plugin "**Patch Management: VMware Go Server Settings**" is selected under “**Plugins**” -> “**Families**” -> “**Settings**”:

**Patch Management: VMware Go Server Settings**
Patch Management: Missing updates from VMware Go

Preferences
Credentials for the VMware Go server must be provided for scanning to work properly.

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Go Server</td>
<td>VMware Go IP address or system name</td>
</tr>
<tr>
<td>VMware Go Domain</td>
<td>The VMware cloud-specified domain the VMware Go server is a part of</td>
</tr>
<tr>
<td>VMware Go Username</td>
<td>VMware Go admin username</td>
</tr>
<tr>
<td>VMware Go Password</td>
<td>VMware Go admin password</td>
</tr>
</tbody>
</table>

In the “Preferences” pane, select “Patch Management: VMware Go Server Settings” from the Plugin drop-down menu:
The following settings pane will be displayed:

Once valid VMware Go credentials have been provided, any of the standard Windows checks will produce output similar to the following:

Microsoft has released a set of patches for SQL Server 2000 and 2005:


Risk Factor: High

**CVSS Base Score**

3.0 (CVSS2#AV:N/AC:L/AU:S/C:C/I:C/A:C)

**CVSS Temporal Score**

7.4 (CVSS2#E:R/FL:O/RC:C)

Plugin Output

The host is missing the patch / patches for MS09-004 according to VMware Go.

**CVE**

CVE-2009-5416

**BID**

32710
RED HAT NETWORK SATELLITE

Red Hat Satellite is a systems management platform for Linux-based systems. Nessus and SecurityCenter have 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 Nessus or SecurityCenter GUI.

Although not supported by Tenable, the RHN 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 the credential 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 Nessus is able to connect to the target system, it will perform checks on that system and ignore RHN Satellite output.
- The data returned to Nessus by RHN 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 two Nessus plugins:

- satellite_settings.nbin (Plugin ID 57063)
- satellite_get_managed_hosts.nbin (Plugin ID 57064)
- satellite_get_packages.nbin (Plugin ID 57065)
- satellite_get_schedule.nbin (Plugin ID 57066)
- satellite_get_system_info.nbin (Plugin ID 57067)

CREATING THE POLICIES

From the Nessus or SecurityCenter web interface, click the "Policies" tab and then "Add". Directions for each tab under the "Add Policy" menu are described in this section.

General

If RHN 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.
**Credentials**
Because RHN Satellite scans do not rely on the system being managed to report patch management issues, credentials for the systems do not need to be used in the scan policy.

**Plugins**
Make sure the following plugins are enabled under “Plugins” -> “Families” -> “Settings”:

- Patch Management: Red Hat Satellite Server Get Installed Packages
- Patch Management: Red Hat Satellite Server Get System
- Patch Management: Red Hat Satellite Server Settings
In addition, enable the local operating system security check plugins of your choice. Nessus currently supports Red Hat Enterprise Server, Fedora, OpenSuSE, and CentOS in conjunction with the Red Hat Satellite Server plugins:

Preferences
Credentials for the RHN Satellite server must be provided for scanning to work properly.
In the "Preferences" pane, select "Patch Management: Red Hat Satellite Server Settings" from the Plugin drop-down menu:

<table>
<thead>
<tr>
<th>Red Hat Satellite server(s)</th>
<th>RHN Satellite IP address or system name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Satellite port(s)</td>
<td>Port Satellite is running on (Typically TCP 80 or 443)</td>
</tr>
<tr>
<td>Red Hat Satellite username(s)</td>
<td>Satellite username</td>
</tr>
<tr>
<td>Red Hat Satellite password(s)</td>
<td>Satellite password</td>
</tr>
</tbody>
</table>

Enter the host, port, user, and password for your Satellite server:

Run the scan. The results of the scan will show which local checks fired:
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Name</th>
<th>Port</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>99952</td>
<td>Patch Management Red Hat Satellite Server Get Installed Packages</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>99959</td>
<td>Patch Management Red Hat Satellite Server Get System Information</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>38806</td>
<td>CentOS : RHSA-2006-0411</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>35310</td>
<td>CentOS : RHSA-2006-0004</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>50004</td>
<td>CentOS : RHSA-2010-0019</td>
<td>general/tcp</td>
<td>High</td>
</tr>
<tr>
<td>53454</td>
<td>CentOS : RHSA-2011-0436</td>
<td>general/tcp</td>
<td>High</td>
</tr>
<tr>
<td>51146</td>
<td>CentOS : RHSA-2010-0078</td>
<td>general/tcp</td>
<td>High</td>
</tr>
<tr>
<td>48303</td>
<td>CentOS : RHSA-2010-0016</td>
<td>general/tcp</td>
<td>High</td>
</tr>
<tr>
<td>43656</td>
<td>CentOS : RHSA-2007-0964</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>44677</td>
<td>CentOS : RHSA-2010-0108</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>44097</td>
<td>CentOS : RHSA-2010-0034</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>43734</td>
<td>CentOS : RHSA-2009-0361</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>43798</td>
<td>CentOS : RHSA-2009-1471</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>34453</td>
<td>CentOS : RHSA-2008-0946</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>43785</td>
<td>CentOS : RHSA-2009-1335</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>43726</td>
<td>CentOS : RHSA-2009-0013</td>
<td>general/tcp</td>
<td>Low</td>
</tr>
<tr>
<td>51885</td>
<td>CentOS : RHSA-2011-0170</td>
<td>general/tcp</td>
<td>High</td>
</tr>
<tr>
<td>47739</td>
<td>CentOS : RHSA-2010-0628</td>
<td>general/tcp</td>
<td>High</td>
</tr>
</tbody>
</table>
ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG and PCI compliance. Tenable’s award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.