

# Tenable.io for Microsoft SCCM

## 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 Microsoft System Center Configuration Manager (SCCM) 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:

Hosts 5
Vulnerabilities 119

INFO
Microsoft Patch Bulletin Feasibility Check
< >

**Description**

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates.

Note that this plugin is purely informational.

**Output**

Nessus is able to test for missing patches using :

Port ^	Hosts
445 / tcp / cifs	172. .53, 172. .152

Nessus is able to test for missing patches using :  
SCCM

Port ^	Hosts
445 / tcp / cifs	172. .33, 172. .74

**Plugin Details**

Severity: Info  
 ID: 57033  
 Version: \$Revision: 1.10 \$  
 Type: local  
 Family: Windows : Microsoft Bulletins  
 Published: 12/06/11 at 12:00 AM  
 Modified: 02/12/16 at 12:00 AM

**Risk Information**

Risk Factor: None

## Microsoft SCCM

SCCM is available from Microsoft to manage large groups of Windows-based systems. Tenable.io has the ability to query the SCCM service to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the Tenable.io UI.

- 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 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.
- Tenable.io connects to the server that is running the SCCM site (e.g., credentials must be valid for the SCCM service, meaning an admin account in SCCM with the privileges to query all the data in the SCCM MMC). This server may also run the SQL database, or the database as well as the SCCM repository can be on separate servers. When leveraging this audit, Tenable.io must connect to the SCCM Server, not the SQL server if they are on separate servers.



Tenable.io SCCM patch management plugins support SCCM 2007 and SCCM 2012.

SCCM scanning is performed using four plugins:

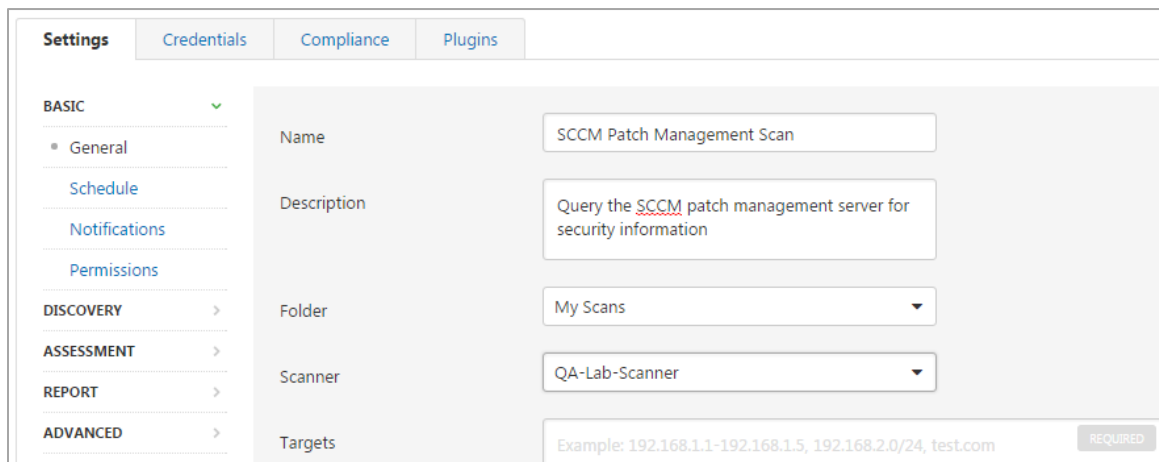
- Patch Management: SCCM Server Settings (Plugin ID 57029)
- Patch Management: Missing updates from SCCM (Plugin ID 57030)
- Patch Management: SCCM Computer Info Initialization (Plugin ID 73636)
- Patch Management: SCCM Report (Plugin ID 58186)

## Creating a Scan

From the Tenable.io web interface, click “**Scans**” and then “**New Scan.**” Select the “**Advanced Network Scan**” template.

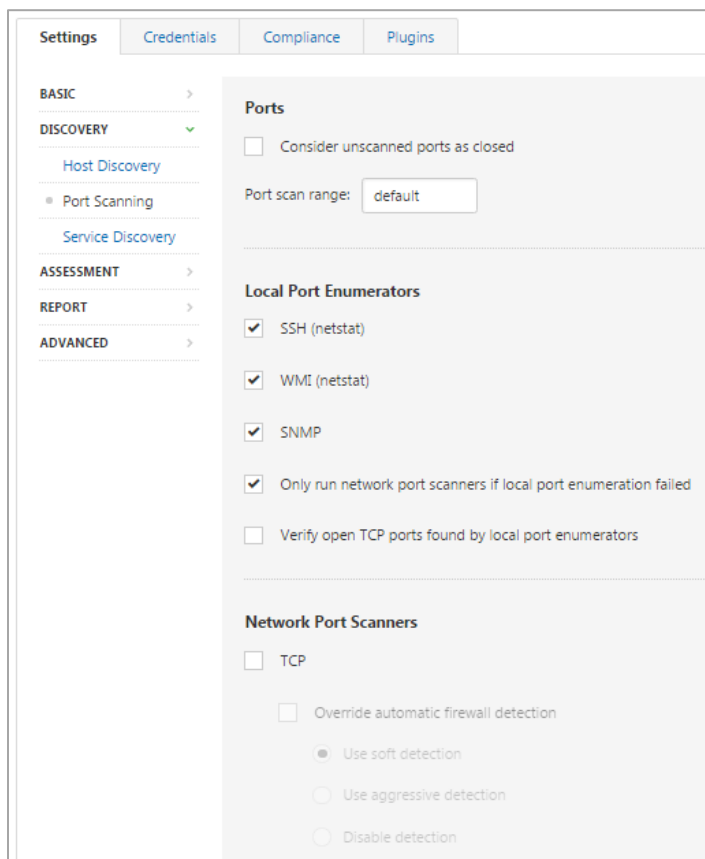
### General Settings

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.



The screenshot shows the 'Settings' page for a scan configuration in the Tenable.io web interface. The page has a navigation bar with tabs for 'Settings', 'Credentials', 'Compliance', and 'Plugins'. The 'Settings' tab is active. On the left, there is a sidebar menu with categories: 'BASIC' (expanded), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. Under 'BASIC', there are sub-items: 'General' (selected), 'Schedule', 'Notifications', and 'Permissions'. The main content area shows the configuration for the 'General' settings:

Name	SCCM Patch Management Scan
Description	Query the <u>SCCM</u> patch management server for security information
Folder	My Scans
Scanner	QA-Lab-Scanner
Targets	Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com <span>REQUIRED</span>



For more information on the options under “Settings,” see the [Tenable.io User Guide](#).

## Plugins

At least four specific plugins must be enabled for the SCCM patch management scans to run. These plugins can easily be found by searching for “SCCM” through the “Plugin Name” advanced filter:

Settings   Credentials   Compliance   <b>Plugins</b>   <a href="#">Show Enabled</a>					
STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	Misc.	3	ENABLED	Patch Management: SCCM Server Settings	57029
ENABLED	Settings	1			
ENABLED	Windows	1			

*Patch Management: SCCM Server Settings*

Settings   Credentials   Compliance   <b>Plugins</b>   <a href="#">Show Enabled</a>					
STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	Misc.	3	ENABLED	Patch Management: Missing updates from SCCM	57030
ENABLED	Settings	1	ENABLED	Patch Management: SCCM Computer Info Initialization	73636
ENABLED	Windows	1	ENABLED	Patch Management: SCCM Report	58186

*Patch Management: Missing updates from SCCM, SCCM Computer Info Initialization, and SCCM Report*

In addition to the SCCM-specific plugins, all plugins in the “**Windows: Microsoft Bulletins**” family must be enabled.

Settings			Credentials	Compliance	Plugins	Show Enabled
ENABLED	Scientific Linux Local Security Checks	2207				
ENABLED	Service detection	423				
ENABLED	Settings	80				
ENABLED	Slackware Local Security Checks	930				
ENABLED	SMTP problems	135				
ENABLED	SNMP	33				
ENABLED	Solaris Local Security Checks	3904				
ENABLED	SuSE Local Security Checks	9516				
ENABLED	Ubuntu Local Security Checks	3537				
ENABLED	VMware ESX Local Security Checks	112				
ENABLED	Web Servers	992				
ENABLED	Windows	3647				
ENABLED	Windows : Microsoft Bulletins	1235				

STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	Microsoft Patch Bulletin Feasibility Check	57033
ENABLED	Microsoft Windows Summary of Missing Patches	38153
ENABLED	MS KB3057154: Update to harden use of DES encryption (3057154)	84763
ENABLED	MS00-029: NT IP Fragment Reassembly Patch Not Applied (jolt2) (259728)	10433
ENABLED	MS00-035: MS SQL7.0 Service Pack may leave passwords on system (2639...	11330
ENABLED	MS00-036: NT ResetBrowser frame & HostAnnouncement flood patch (26...	10434
ENABLED	MS00-047: NetBIOS Name Server Protocol Spoofing patch (269239)	10482
ENABLED	MS00-052: Relative Shell Path patch (269049)	10486
ENABLED	MS00-053: Service Control Manager Named Pipe Impersonation patch (26...	10485
ENABLED	MS00-062: Local Security Policy Corruption (269609)	10499
ENABLED	MS00-065: Still Image Service Privilege Escalation patch (272736)	10504
ENABLED	MS00-066: Malformed RPC Packet patch (272303)	10509
ENABLED	MS00-067: Telnet Client NTLM Authentication Vulnerability (272743)	10519

Windows: Microsoft Bulletins

## Preferences

Credentials for the SCCM system must be provided for SCCM scanning to work properly. Under the “**Credentials**” tab in Tenable.io, select “**Patch Management**” and then “**Microsoft SCCM**”:

Settings	Credentials	Compliance	Plugins
CLOUD SERVICES			
DATABASE			
HOST			
MISCELLANEOUS			
MOBILE			
PATCH MANAGEMENT			
Dell KACE K1000			1
IBM Tivoli Endpoint Manager (BigFix)			1
Microsoft WSUS			1
Red Hat Satellite 6 Server			1
Red Hat Satellite 5 Server			∞
Symantec Altiris			1
PLAINTEXT AUTHENTICATION			

Microsoft SCCM	
Server	sccm.example.org
Domain	CYCLONE
Username	administrator
Password	.....

Save Cancel

Credential	Description
SCCM Server	SCCM IP address or system name
SCCM Domain	The domain for the SCCM server
SCCM Username	SCCM admin username
SCCM Password	SCCM admin password

Tenable.io will report on where SCCM detects an unmanaged system that does not have the client installed:

INFO

Patch Management: SCCM Report

Plugin Details

---

**Description**

This plugin parses the patch information from the SCCM server provided in order to determine if the system scanned is managed by the SCCM server. If so, the plugin then determines which patches are missing from the target system.

This plugin will use the information provided from the SCCM server to generate a report that can be viewed once the scan is complete.

**Output**

```
This system is not managed or has not checked in properly with SCCM.
```

Port	Hosts
N/A	172.16.1.45

Severity: Info

ID: 58186

Version: \$Revision: 1.36 \$

Type: local

Family: Misc.

Published: 03/01/12 at 12:00 AM

Modified: January 16 at 12:00 AM

---

**Risk Information**

Risk Factor: None

When reporting system findings, Tenable.io will report that the information came from SCCM:

**CRITICAL** MS14-026: Vulnerability in .NET Framework Could Allow Elevatio... >

---

**Description**  
The remote Windows host has a version of the Microsoft .NET Framework that is affected by a privilege escalation vulnerability due to the way that .NET Framework handles TypeFilterLevel checks for some malformed objects.

Note that this vulnerability only affects applications that use .NET Remoting.

**Solution**  
Microsoft has released a set of patches for .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4.0, 4.5, and 4.5.1.

**See Also**  
<https://technet.microsoft.com/library/security/MS14-026>

**Output**

```
The following patch management products report :
SCCM : Vulnerable

*Nessus did not run local checks.
```

Port ^	Hosts
445 / tcp / cifs	172.17.0.33, 172.17.0.74

---

**Plugin Details**

Severity: Critical  
ID: 73985  
Version: \$Revision: 1.11 \$  
Type: local  
Family: Windows : Microsoft Bulletins  
Published: 05/14/14 at 12:00 AM  
Modified: 07/01/16 at 12:00 AM

---

**Risk Information**

Risk Factor: Critical  
CVSS Base Score: 10.0  
CVSS Temporal Score: 7.8  
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/IC:A/C  
CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

---

**Vulnerability Information**

CPE: cpe:/a:microsoft:.net\_framework  
Exploit Available: true  
Exploit Ease: Exploits are available  
Patch Pub Date: 05/13/14 at 12:00 AM

Additionally, Tenable.io can query the SCCM system to determine which patches are not installed:

**INFO** Patch Management: SCCM Report

**Description**

This plugin parses the patch information from the SCCM server provided in order to determine if the system scanned is managed by the SCCM server. If so, the plugin then determines which patches are missing from the target system.

This plugin will use the information provided from the SCCM server to generate a report that can be viewed once the scan is complete.

**Output**

```
+ System Information
- Computer Name : RE-SCCM2K12-SQL
- NetBIOS Name : RE-SCCM2K12-SQL
- OS : Microsoft Windows NT Advanced Server 6.1
- Caption : Microsoft Windows Server 2008 R2 Enterprise
- System Type : x64-based PC
- Model : VMware Virtual Platform
- Creation Date : 12/06/2013 20:51:27

- IP Addresses : 
- Domain : 
- Gateway : 
- Subnet : 255.255.252.0
- MAC Address : 00:50:56:BD:1C:04

- Last User : administrator
- Last User Domain :

- Is Client Installed : yes
- Client Version : 5.00.7804.1000
- Status : OK

+ Missing Update List
+ Update for Windows Server 2008 R2 x64 Edition (KB2798162)
- Bulletin : 
- KB : 2798162
- Last Checked : 12/15/2016 19:18:40

+ Security Update for Windows Server 2008 R2 x64 Edition (KB2813430)
- Bulletin : 
- KB : 2813430
- Last Checked : 12/15/2016 19:18:10

+ Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems
```

## 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](https://tenable.com).