Tenable.io for Microsoft SCCM

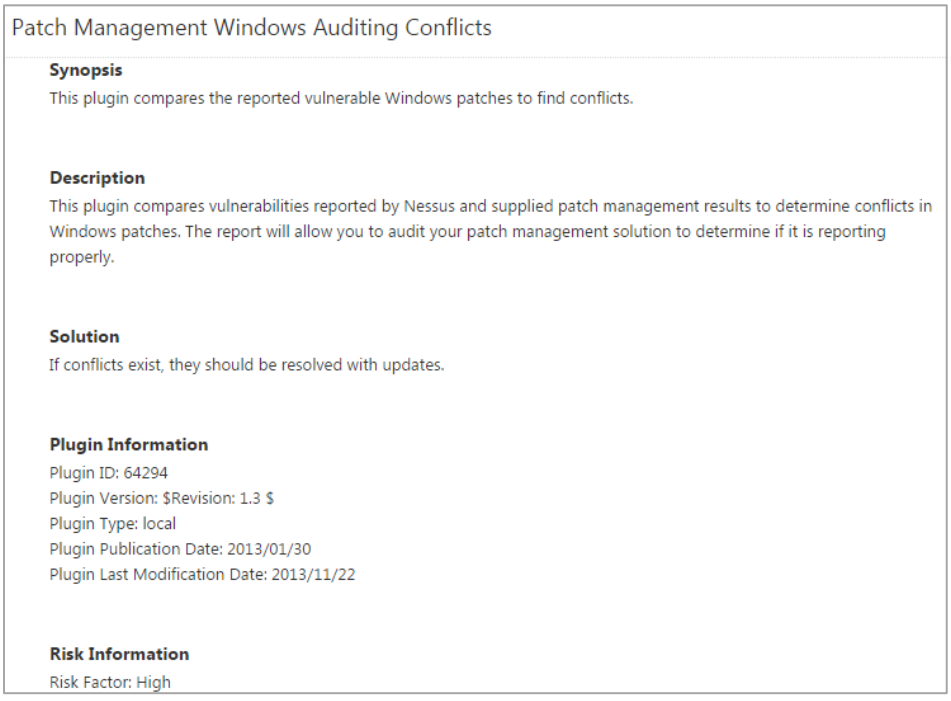
Introduction

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

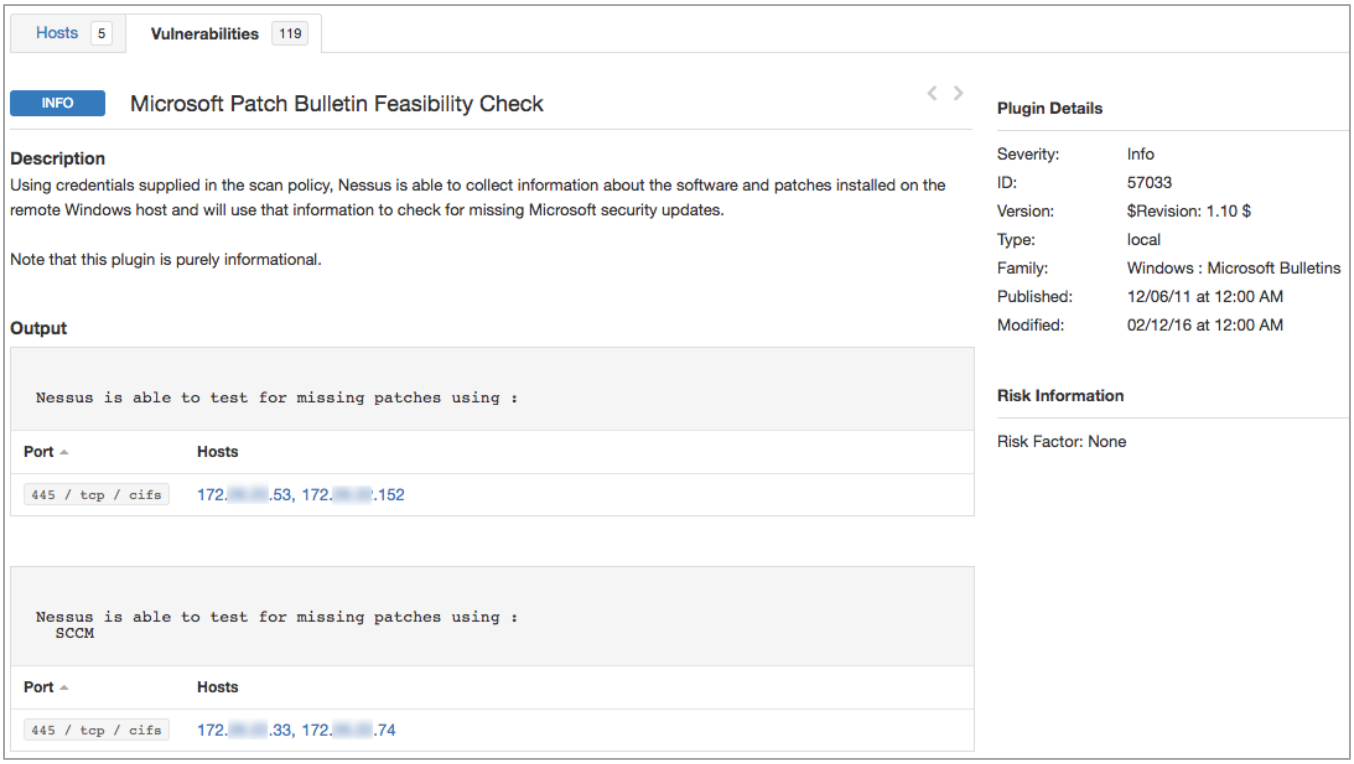
Plugin ID: 64294
Plugin Version: $Revision: 1.3 $
Plugin Type: local
Plugin Publication Date: 2013/01/30
Plugin Last Modification Date: 2013/11/22

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:



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.

Copyright 2017 Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. Tenable and Tenable.io are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners. EN-JUN82017-V2

SCCM scanning is performed using four plugins:

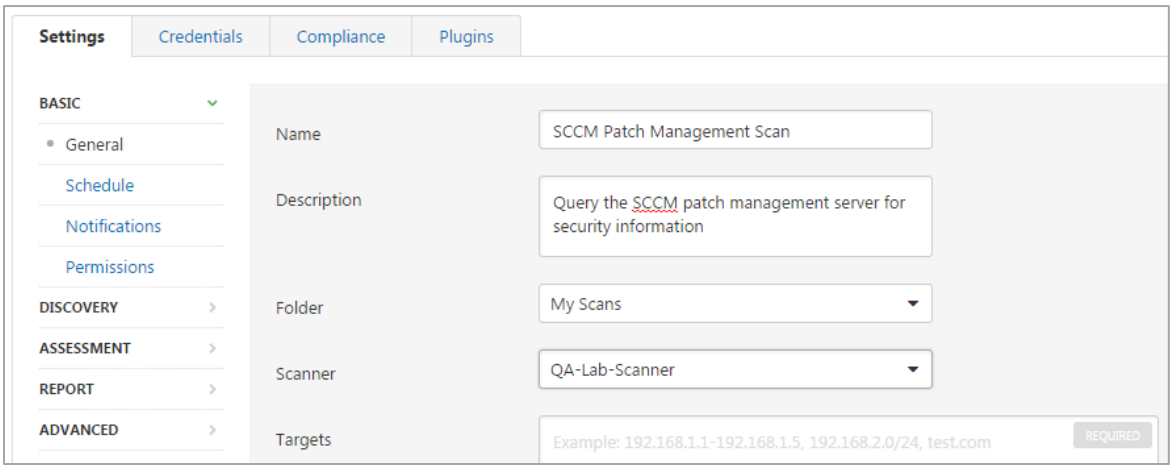
- Patch Management: SCCM Server Settings (Plugin ID 57029)
- Patch Management: Missing updates from SCCM (Plugin ID 57030)
- Patch Management: SCCM Computer Info Initialization (Plugin ID 73636)
- Patch Management: SCCM Report (Plugin ID 58186)

Creating a Scan

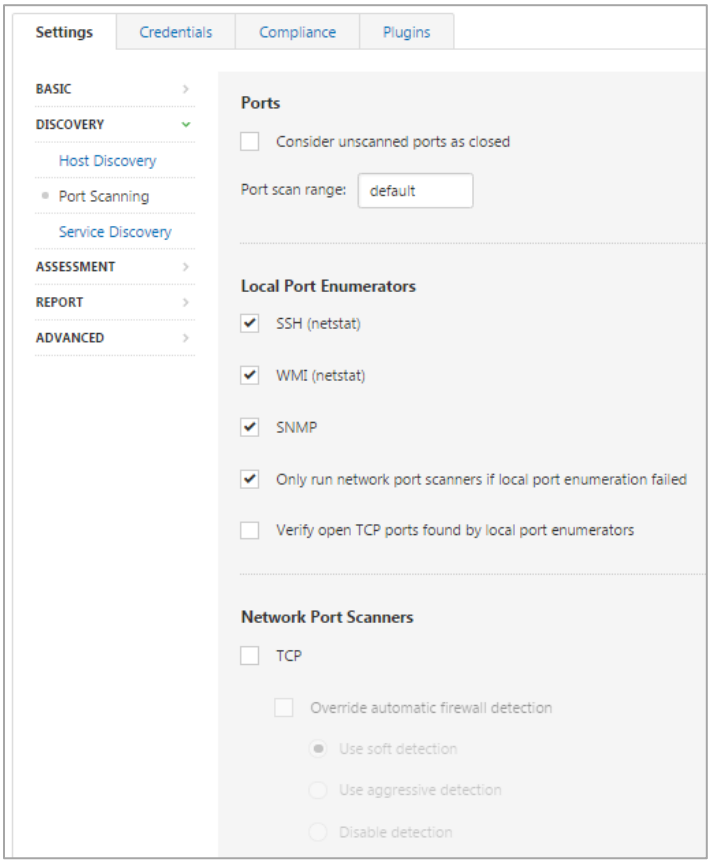
From the Tenable.io web interface, click "**Scans**" and then "**New Scan**." Select the "**Advanced Network Scan**" template.

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.



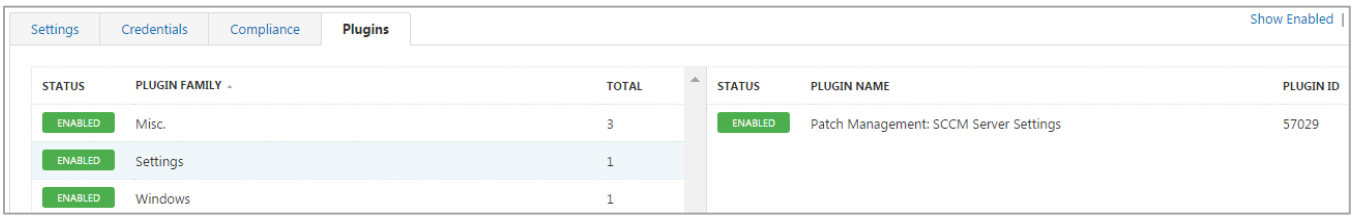
Copyright 2017 Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. Tenable and Tenable.io are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners. EN-JUN82017-V2



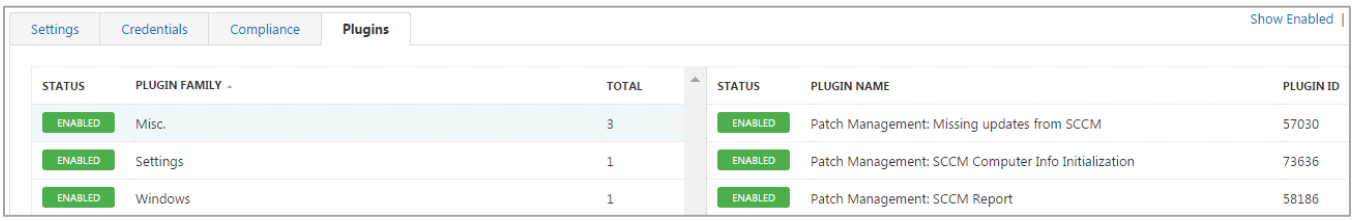
For more information on the options under "**Settings**," see the Tenable.io User Guide.

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:



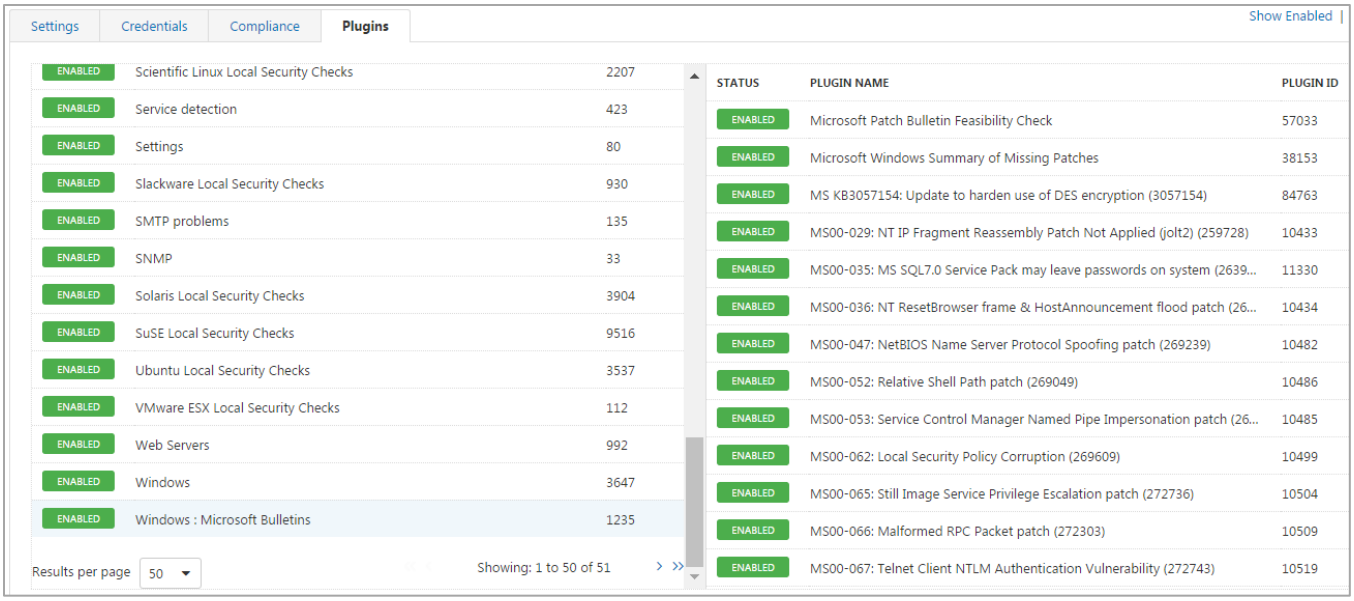
Patch Management: SCCM Server Settings



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

Copyright 2017 Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. Tenable and Tenable.io are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners. EN-JUN82017-V2

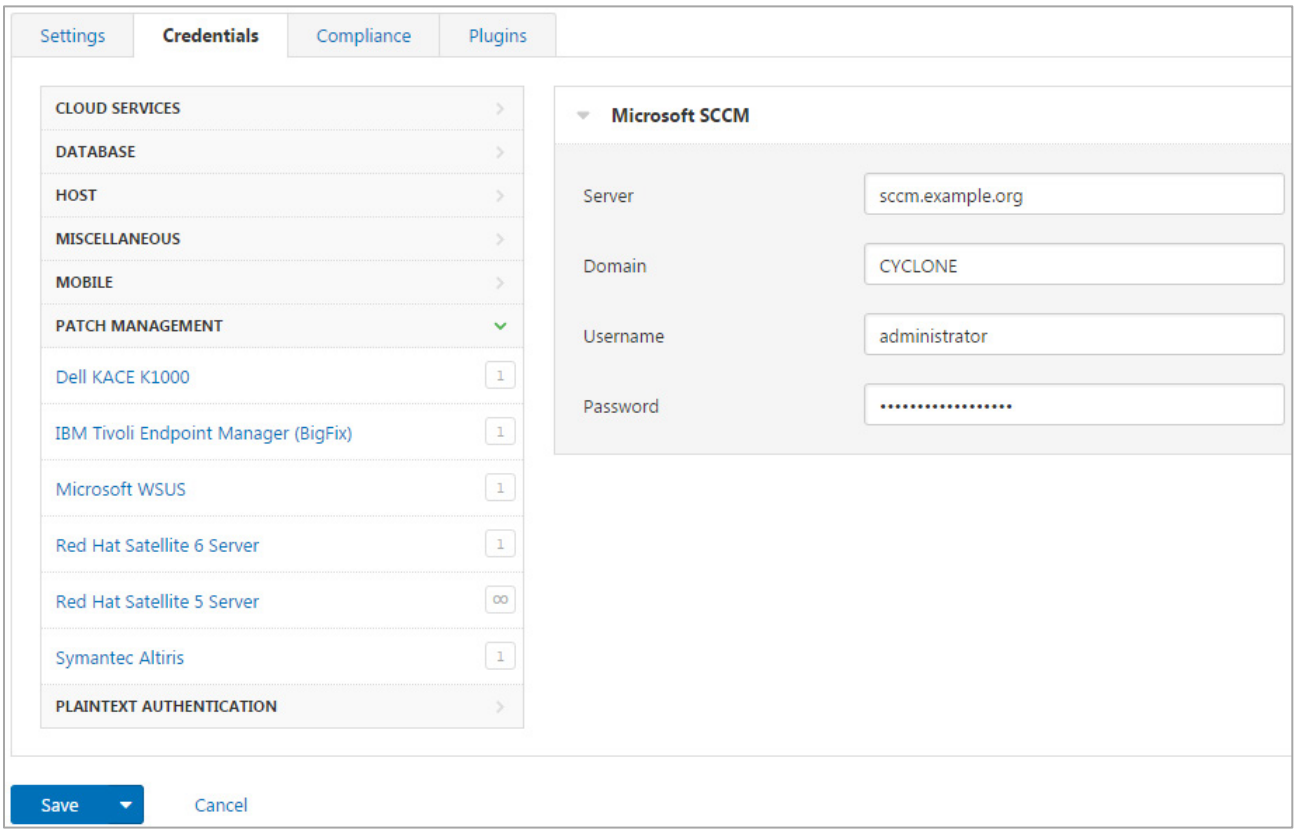
In addition to the SCCM-specific plugins, all plugins in the "**Windows: Microsoft Bulletins**" family must be enabled.



Windows: Microsoft Bulletins

Preferences

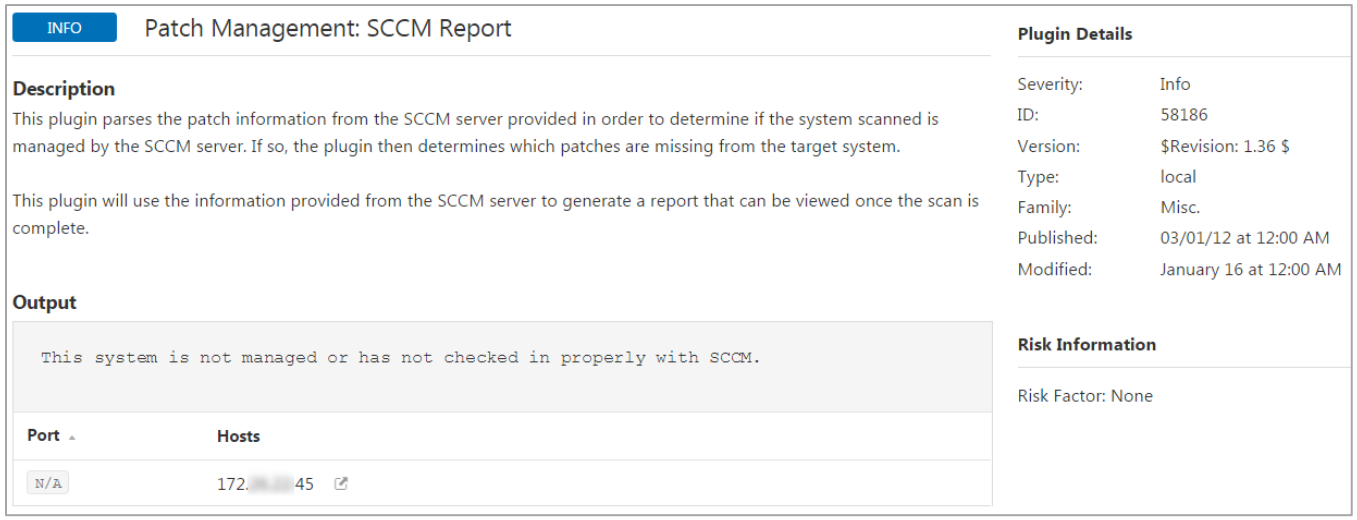
Credentials for the SCCM system must be provided for SCCM scanning to work properly. Under the "**Credentials**" tab in Tenable.io, select "**Patch Management**" and then "**Microsoft SCCM**":



Copyright 2017 Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. Tenable and Tenable.io are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners. EN-JUN82017-V2

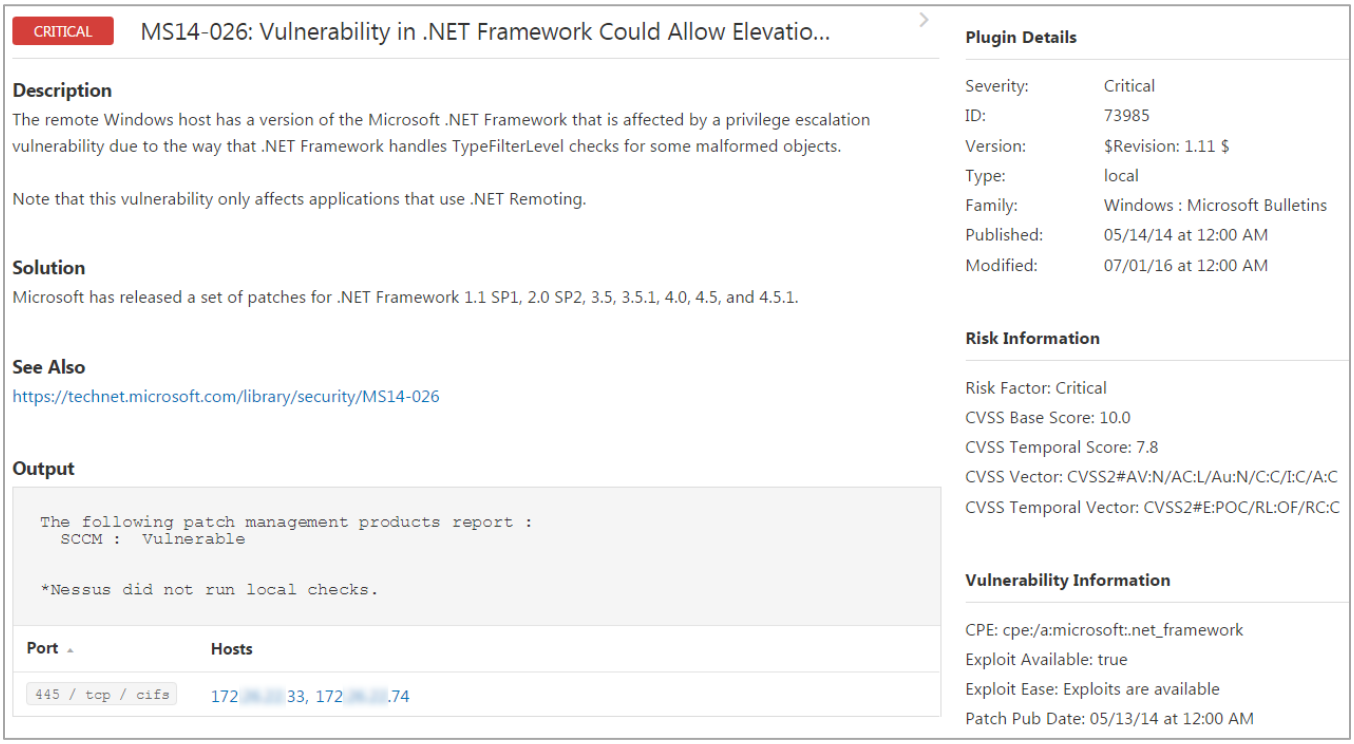
Credential	Description
SCCM Server	SCCM IP address or system name
SCCM Domain	The domain for the SCCM server
SCCM Username	SCCM admin username
SCCM Password	SCCM admin password

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



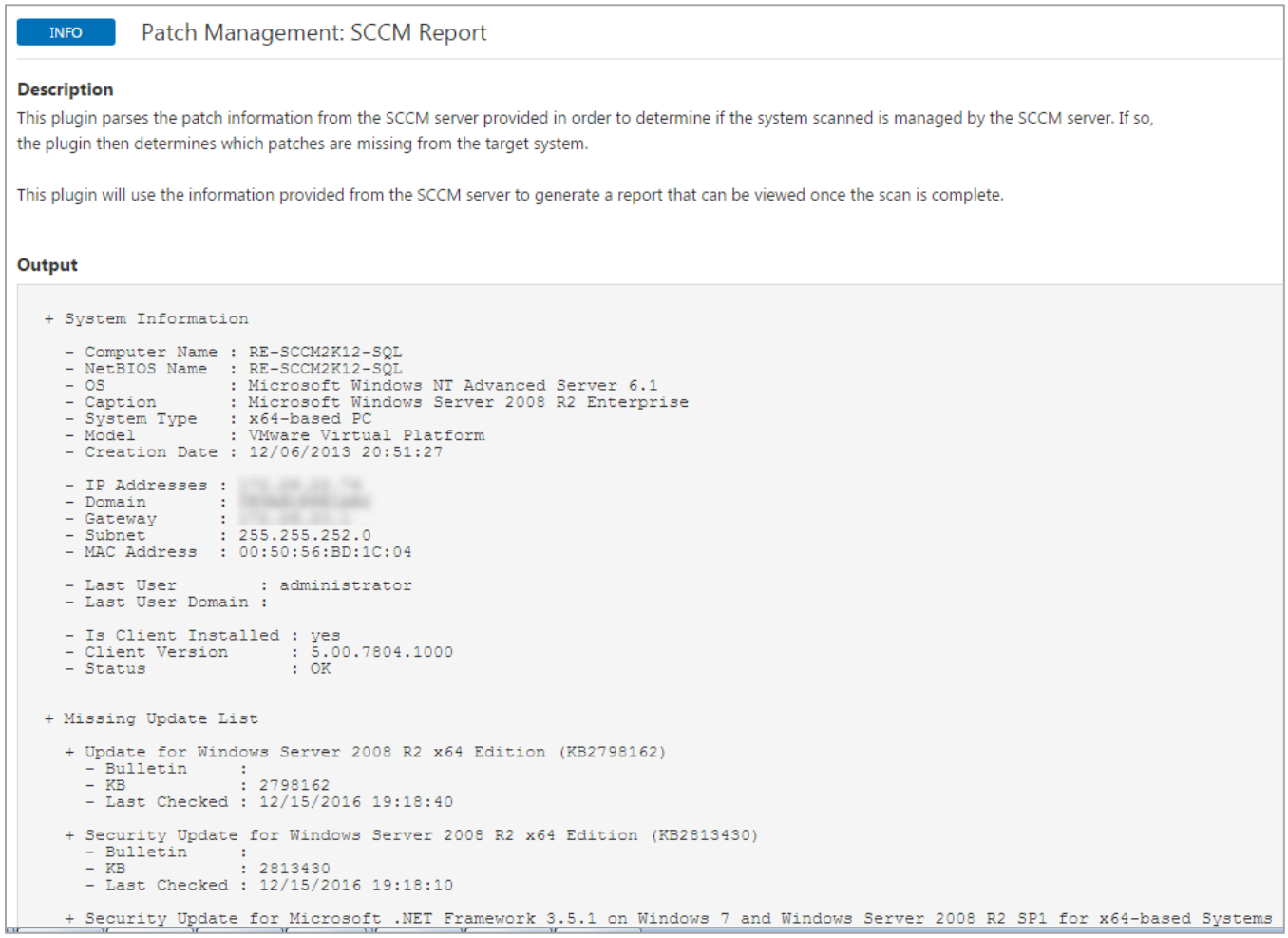
Copyright 2017 Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. Tenable and Tenable.io are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners. EN-JUN82017-V2

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



Copyright 2017 Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. Tenable and Tenable.io are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners. EN-JUN82017-V2

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



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.

Copyright 2017 Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. Tenable and Tenable.io are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners. EN-JUN82017-V2