Secunia
Stay Secure

Complete Patch Management

Targeted, Reliable and Cost-efficient

Secunia CSI

Corporate Software Inspector

Secunia
Stay Secure

Empower your IT-Operations and Security Teams with the most reliable Vulnerability & Patch Management solution to eliminate the Vulnerability Threat

Secunia CSI 6.0 Combines Vulnerability Intelligence, Vulnerability Scanning, and Patch Creation with Patch Deployment Tool Integration to Enable Targeted, Reliable, and Cost-efficient Patch Management

The Secunia CSI 6.0 is a vulnerability and patch management solution that completes the patch management process. It provides the reliable, comprehensive, and up-to-date Vulnerability Intelligence and highly accurate scan results needed by IT-operations and Security teams to proactively deal with the Vulnerability threat imposed by unpatched programs.

By combining reliable Vulnerability Intelligence and Vulnerability Scanning with automated Patch Creation and integration with your patch deployment solution, the intelligence becomes actionable in a Client Management (CM), Security Information & Event Management (SIEM), and Governance, Risk & Compliance (GRC) perspective. Further, remediation efforts become more targeted, ensuring that IT and Security Officers are focusing on the vulnerabilities that have the greatest impact on the organisation's security state.

The Secunia CSI assesses the security state of practically all legitimate programs running on Microsoft Windows platforms and supports scanning of Windows, Apple Mac OSX, Red Hat Enterprise Linux (RHEL) platforms and custom software. It integrates with Microsoft WSUS & SCCM and third-party client management tools for easy deployment of third-party updates, making patching a simple and straight-forward process for all IT departments.

By integrating the Secunia CSI into your infrastructure you are able to:

- Get an overview of installed programs across endpoints and servers
- Scan and patch non-Microsoft programs
- Pinpoint the exact vulnerabilities affecting the network (location and criticality)
- Receive real-time alerting upon security changes
- Prioritize patching efforts according to the risk exposure
- Optimise package creation

CSI 6.0 HIGHLIGHTS

- Scanning of Red Hat Enterprise Linux
- Custom scan rules
- Secunia Smart Groups and Smart Group notifications
- Integration with third-party patch deployment solutions
- Integration with Microsoft SCCM for agent-less scanning
- Active Directory integration

The Intelligence

The Secunia CSI sources the Secunia Advisory & Vulnerability Database to assess the security state of the identified programs. Secunia offers the industry's largest Vulnerability Intelligence database where every vulnerability has been verified, assessed, corrected, and tested by a Secunia Research Specialist, before an advisory is published.

The database covers both old and new vulnerabilities, ensuring a complete and comprehensive overview of the security state of the infrastructure's install base. The Vulnerability Intelligence provided for each identified program is highly detailed, revealing criticality rating, exposure time, and status (Insecure, End-of-Life or Patched).

The Technology

The proprietary Secunia Software Inspector technology relies on an authenticated scan approach, which enables the Secunia CSI to identify all installed programs and plug-ins based on the actual files present on the system. It correlates program metadata with Secunia's comprehensive product database to build an inventory of the installed programs and plug-ins. This inventory is then correlated with vulnerability metadata based on Secunia Vulnerability Intelligence. This is an extremely reliable mapping approach and removes the flaw in identifying false-positives.

The Level Of Scan
There are three different scan levels that are available for you to choose.

- **Type 1.** Scans for programs in default paths.
- **Type 2.** Scans for programs on all local hard drives in all paths.
- **Type 3.** Scans all *.EXE, *.OCX, *.DLL and other relevant program files on all local hard drives.

The Type Of Scan
The Secunia CSI offers various scanning options designed to suit your environment:

Agent-less scanning of your systems can be performed out-of-the box. When running agent-less, the Secunia CSI utilises standard Windows networking services to scan the systems on your network. The agents can also be automatically deployed through the Microsoft WSUS/SCCM integration.

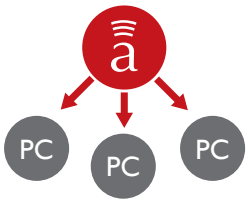
Agent-based scanning is more flexible. It can be used in segmented networks and to scan systems that are not always online (e.g. laptops). The agents can also be automatically deployed through the Microsoft WSUS/SCCM integration.

Appliance mode offers "agent-less" scanning from centralised hosts; in branch offices for example. Command Line Interface mode makes it possible to schedule and manage scans using other tools (e.g. log-on scripts).

The Patch Management Process

The Patch Management process works by looking at the actual files on the system being scanned. The result is extremely reliable as a program cannot be installed on a system without the actual files required being present.

1

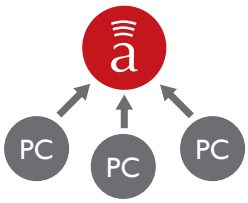


The Secunia CSI scans computers in your network from a central location

2

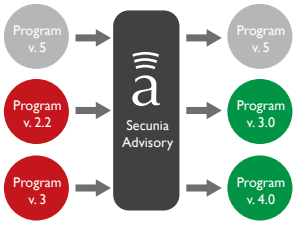
It scans all executables, including EXE, OCX, and DLL files

3



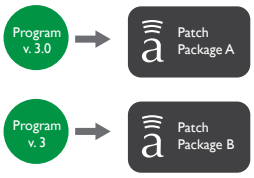
All scan results are fed into the central management console for easier analysis to give a complete overview of what is installed.

4



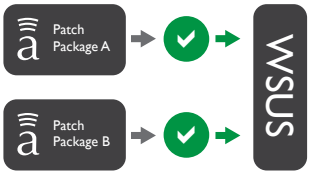
The Secunia CSI tells you which version to update

5



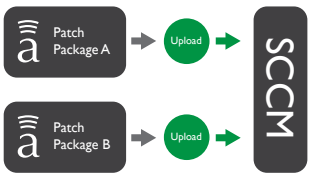
Automatic repackaging

6a



Deploy patch to WSUS and verify application

6b



Deploy patch to SCCM and verify application

The Core Benefits

Patch Creation

Packages are delivered out of the box for a number of programs, including those where the vendor does not offer silent installation parameters. The packages are created by Secunia Research Team.

Patch Deployment

The Secunia CSI provides simple methods for repackaging and publishing patches for distribution via for example Microsoft WSUS. This third-party integration for patching is enabled through the SDK.

The Secunia CSI can further conduct scans of desktop and server systems to ensure that updates are applied correctly and that all systems are fully compliant.

Performance

Small system footprint ensuring short scan times, smooth performance, and no limitation to the amount of scanned hosts.

Reporting

The Secunia CSI's customisable dashboard gives you a complete overview of the security and compliance state of your entire corporate network, enabling you to access and organise all data and results from a single location.

- Smart Group Notifications
- Scheduled Data Export (API)
- Activity Log

Configuration

- Active Directory Integration
- IP Access Management
- Secunia VIM 3 Integration
- Secunia PSI 3.0 Integration

Scope

The Secunia CSI can detect any type of software or plug-in as long as it has the correct version information from the vendor.

Further, it is capable of assessing the security state of practically all legitimate programs running on Microsoft Windows platforms. It supports scanning of Windows, Apple Mac OSX, Red Hat Enterprise Linux (RHEL) platforms, and custom software.

System Requirements

Supported Microsoft Operating Systems:
Windows XP SP2 or later
Windows Vista
Windows 7
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2

Running the centralised dashboard

- Network/Internet connection (SSL 443/tcp to csi.secunia.com)
- 10 MB of free disk space

On demand and Appliance scanning

- Network/Internet connection (SSL 443/tcp to csi.secunia.com)
- Administrative privileges on target hosts
- Windows Update Agent 2.0 or later
- Workstation and Server Service started
- Remote Registry Service started
- File and Print Sharing enabled
- COM+ started
- Ports 139/tcp and 445/tcp open inbound

Local Agent based scanning

- Network/Internet connection (SSL 443/tcp to csi.secunia.com)
- Local administrative privileges
- 1 MB of free disk space

Support And Maintenance

All support questions should be addressed to the Secunia Customer Support Center

csc@secunia.com

A number of support and information resources have also been made available:

User Forums
Interact with other users by posting questions or submitting tips.

Product Documentation
Review product specifications, getting started guides and more.

Product guide
In the Secunia CSI solution

Try Secunia CSI today!
Sign up for a FREE trial by scanning this QR-code.

Feature Overview

Microsoft WSUS Integration

The Secunia CSI integrates seamlessly with Microsoft Windows Server Update Services (WSUS) for easy deployment of third-party updates. This makes installing updates simple and straightforward due to the automatic repackaging feature and the Microsoft WSUS distribution management functionality in the Secunia CSI.

Microsoft SCCM Integration

The Secunia CSI integrates seamlessly with Microsoft System Center Configuration Manager (SCCM) 2007 and 2012 to help you stay compliant and up-to-date with the latest security updates from third-party vendors and Microsoft. Organisations that use MS SCCM already have agents installed on the endpoints in their environment. Instead of installing an additional agent from Secunia, these can now configure the SCCM software inventory agent to handle the scanning, which means one less agent on all their endpoints.

Third-party Integration for Patching

The Secunia CSI can now be easily integrated with your preferred patch deployment solution (for example, the Altiris Deployment Solution) using the Secunia Patch Deployment SDK to allow for easy patch management (patch scanning, patch creation and patch deployment).

Secunia Smart Groups

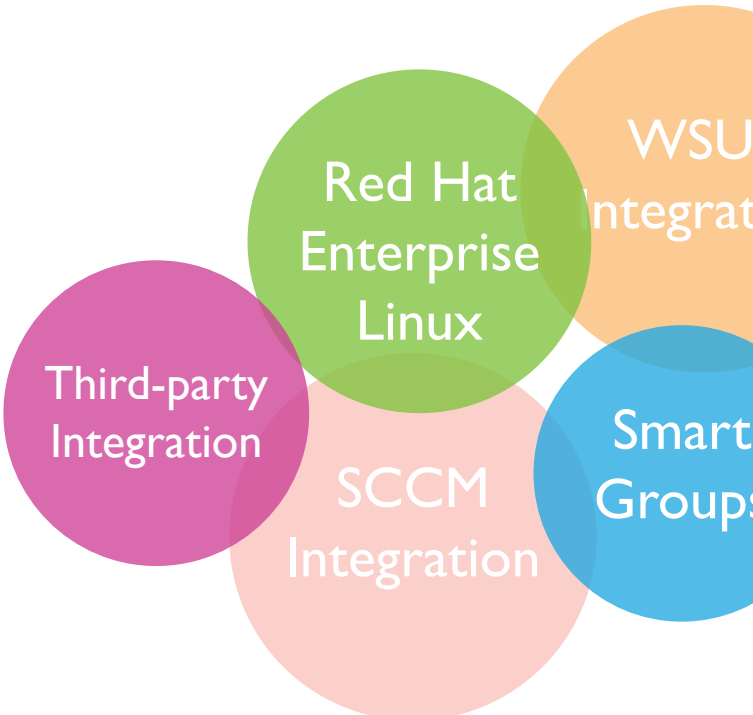
Secunia Smart Groups help you prioritize your remediation efforts and stay secure and compliant by allowing you to filter and segment your data. This means that you can focus on what is relevant for you to reduce risk, stay compliant, increase the Return on Security Investment (ROSI), or whatever metrics are relevant for you.

Smart Group Notifications

Configure email notifications and SMS alerts, so that you are immediately notified when an event occurs that is relevant to you. You might want to know if a highly critical vulnerability is not being patched within 30 days (as required to be PCI-DSS compliant), or you might want to be notified every time an extremely critical advisory is issued that is relevant for your environment.

Scanning Red Hat Enterprise Linux (RHEL)

The Secunia CSI 6.0 has expanded coverage to also include scanning of Red Hat Enterprise Linux in addition to Windows and Mac OSX. Hence, users will be able to extensively cover their devices and get an even more comprehensive overview of programs and vulnerabilities in their environment with the Secunia CSI. Users can view and export the Red Hat Enterprise Linux inventory. The scan agent (Perl) for RHEL uses the inventory which is already present (RPM) and displays this in the CSI after being processed by Secunia Detection/Version Rules.



Custom Software Scanning
The Secunia CSI can now be used to scan custom software. That is, if you have (non-public) software that has been designed for your organisation, you can use the Secunia CSI to identify exactly on which hosts this is present, and deploy updates using the Secunia Package System (SPS) together with your existing deployment solution.

Scheduled Data Export
Use the Exporting function to schedule automatic exports of data, for example data required to be automatically imported into a GRC tool for compliance purposes.

Active Directory Integration
Automatically update organisational units and structure in the Secunia CSI when changes are made to the Active Directory, and avoid double-work and ensure that your environment is always in sync.

Activity Log
View a full log of all activities in the Secunia CSI, including "write" actions, logins, and so on. This is, for example, valuable for compliance and auditing purposes or for troubleshooting or investigating specific incidents.

IP Access Management
Use the IP Access Management window to configure the IP addresses the Secunia CSI console can be accessed from, thereby further limiting the risk of unauthorized access to the console and your environment.

Integration with Secunia PSI 3.0
Integration with Secunia PSI 3.0 allows you to also manage PCs that are not regularly connected to your network. The Secunia PSI 3.0 provides automatic updating and a simple user interface available in multiple languages, thereby making PC maintenance a straight forward and easy task for all users with administrative privileges on their PCs. It gives administrators access to scan results from the PCs that are not directly under their control, and they are able to approve security updates on these PCs.

Integration with Secunia VIM
Integration with the Secunia Vulnerability Intelligence Manager (VIM) allows for automatically creating and updating asset lists in the Secunia VIM based on the Secunia CSI scan results, thereby allowing for easily tracking vulnerability management efforts and compliance reporting.

Secunia
Stay Secure

About Secunia

Secunia is the leading provider of IT security solutions that help businesses and private individuals globally manage and control vulnerability threats and risks across their networks and endpoints.

Secunia plays an important role in the IT security ecosystem, and is the preferred supplier for enterprises and government agencies worldwide, counting Fortune 500 and Global 2000 businesses among our customer base.

Contact

For further information about Secunia's competencies, please contact sales@secunia.com

Stay Secure.

Try Secunia CSI today!
Sign up for a FREE trial by scanning this QR-code.

facebook.com/secunia gplus.to/secunia twitter.com/secunia linkedin.com/company/secunia

Visit us at **secunia.com**