Complete Patch Management
Complete - Flexible – Unique

Secunia CSI 7
Corporate Software Inspector
Take control of the vulnerability threat and optimize your IT security investments. The Secunia CSI gives you the **when**, the **where**, the **what** and the **how**.

The Secunia CSI 7.0 combines scanning and patching, thereby meeting the requirements of both IT security and IT operations. This combination of vulnerability intelligence, vulnerability scanning, patch creation and patch deployment integration is unique in the industry.

The Secunia CSI 7.0 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 organization’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), Android 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 alerts upon security changes
- Prioritize patching efforts according to the risk exposure
- Optimize package creation

**CSI 7.0 HIGHLIGHTS**

- Smart Groups 2.0
- Patch Configuration
- User Management
- Web Console (SaaS)
- Live Update
- PSI for Android
- Password Policy Configuration

**Add-ons**

- Secunia SC2012 Plugin
- Zero-Day Vulnerability Support
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 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, and reveals for example 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 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 utilizes 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 centralized 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).

**System Center Configuration Manager Inventory Import** scan results are obtained from the data collected by the System Center Configuration Manager software inventory agent, which avoids the need to install the Secunia CSI agent on each client.
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. Deploy patch to WSUS or 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 and tested by the 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 customizable dashboard gives you a complete overview of the security and compliance state of your entire corporate network, enabling you to access and organize 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
- Secunia PSI for Android Integration
- Patch Configuration

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) and Android platforms, and custom software.
System Requirements

To use the Secunia CSI 7.0 Console your system should meet the following requirements:

- Min resolution: 1024x768
- The latest version of an Internet browser such as:
  - Internet Explorer (recommended)
  - Firefox (PC, Mac)
  - Safari
  - Chrome
  - Opera (PC, Mac)
- Internet connection capable of connecting to https://csi7.secunia.com
- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
- A PDF reader (for example, Adobe Reader) – optional

The Secunia CSI 7.0 with Patching Capability

To successfully create updates the following should also be present when using the Secunia CSI:

- The latest version of Internet Explorer with the CSI Plugin
- WSUS installer (Administration console only)
- Visual C runtime
- Microsoft .NET Framework runtime 4 or later
- If the WSUS Self-Signed Certificate is going to be used, and the user wishes to provision the certificate through the Patching > WSUS/SCCM > Deployment function, Remote Registry service must be enabled on the clients
- Select the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection), right-click and select Verify and Install Certificate

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
What's new in Secunia CSI 7.0?

Scanning and Reporting

Zero-Day Vulnerability Support (Add-on)
Get access to zero-day advisories that are relevant for your environment based on your scan results, and be alerted via SMS or email whenever a new zero-day vulnerability is discovered that affects your infrastructure.

PSI for Android
Scan your mobile devices running Android for application vulnerabilities with the Secunia PSI for Android, and integrate this with the Secunia CSI to get a full overview of the security status of all devices in your network, for example to support your Bring Your Own Device (BYOD) policy.

Smart Groups 2.0
Easily filter and segment your data to prioritize what is important for you based on Products, Devices or Advisories. Create and schedule on-demand reports based on these Smart Group filters. Receive email notifications and SMS alerts to be immediately notified when an event occurs that is relevant to you.

Patching

Patch Configuration
Get configurable patches out-of-the-box that can be easily customized to support your environment, for example to avoid desktop shortcuts and prompting users to accept an EULA when deploying new updates.

Secunia SC2012 Plugin 2.0 (Add-on)
Get access to all third-party updates directly in Microsoft System Center 2012 via the Secunia SC2012 Plugin, and use your predefined collections in Microsoft System Center 2012 for scheduling custom scans of your infrastructure.

Infrastructure and Configuration

Account Management
Create user accounts with different roles and permissions, thereby allowing these users to only access the data (for example based on an IP range or your Active Directory) and modules (for example Scanning, Reporting and Patching) that are relevant for them.

Web Console (SaaS)
Log in to the Secunia CSI from any internet browser for instant access to your data and reports - anywhere, at any time. Please note that for some modules (for example Patching) to work, a browser plugin is required. This is currently available for Internet Explorer.

Live Update
Get an immediate overview of how a new vulnerability affects your infrastructure based on your latest scan results as soon as the advisory has been released by Secunia Research – no more waiting for the next scanning to take place.

Password Policy Configuration
Determine and enforce the global password policy for your organization to comply with internal and external policies as well as to meet best-practice standards in your industry.
Other CSI Features

**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. Organizations that use Microsoft SCCM already have agents installed on the endpoints in their environment. Instead of installing an additional agent from Secunia, these can 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 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).

**Scanning Red Hat Enterprise Linux (RHEL)**
The Secunia CSI 7.0 includes scanning of Red Hat Enterprise Linux in addition to Windows and Mac OSX. Consequently, 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.

**Custom Software Scanning**
The Secunia CSI can be used to scan custom software. That is, if you have (non-public) software that has been designed for your organization, 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 organizational units and structure in the Secunia CSI when changes are made to the Active Directory, 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 useful for e.g. compliance and auditing purposes, and 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 straightforward and easy task for all users with administrative privileges. 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.
About Secunia

Secunia is a 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.