

# Secunia Corporate Software Inspector

## Inspect, identify, and remediate vulnerabilities

**"98 out of 100 PCs that are connected to the Internet have insecure programs installed!"**

*Secunia PSI user statistics, December 2008*

**"The customers are requesting solutions which can bridge the gap between vulnerability management and deployment of patches... So far, we have not seen any companies offering such a solution"**

*Gartner analysts, IT Security Summit, 2008*

### Scan your network for vulnerabilities

The Secunia Corporate Software Inspector (CSI) is a revolutionary tool that simplifies the troublesome area of identifying vulnerable programs and patching them.

By scanning the network, organisations can effectively protect their corporate IT infrastructure against the threat posed by unpatched vulnerabilities.

With the CSI, keeping your network secure has never been easier.

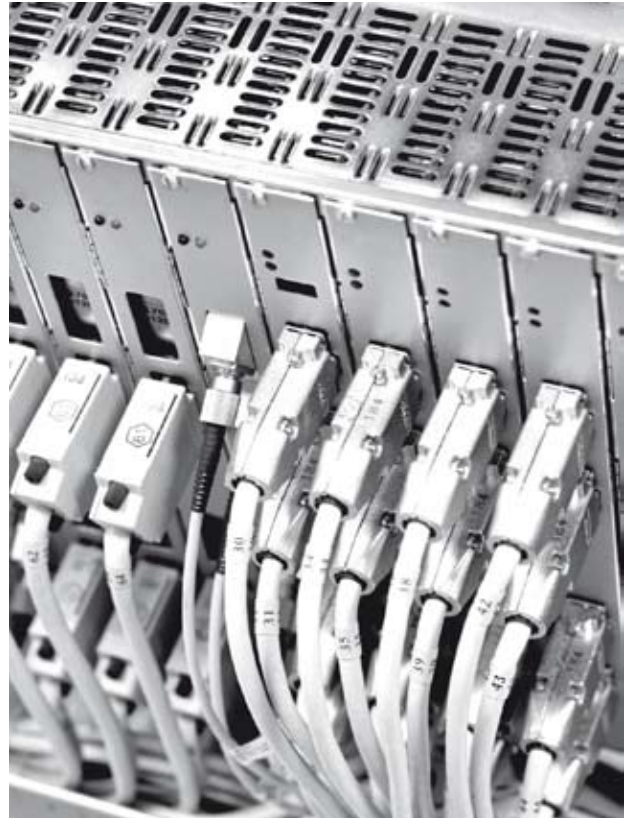
The vulnerability issue cannot be denied. Every corporation faces the certain knowledge that vulnerabilities in the IT infrastructure can and will be used to compromise security. This represents extra challenges for the persons responsible for IT:

- How can you protect your IT infrastructure more effectively?
- How can you make sure that your network does not have any installed software with missing patches?
- How can you do this without using vast amounts of time and effort checking dozens of vendor sites for software updates?

### What are the benefits?

The CSI enables the responsible IT security personnel to gain a complete overview of the corporate network. It pinpoints exact vulnerabilities affecting the network, and gives an in-depth, concise view and resolution of the vulnerability, indicating the location of the threat as well as guidance for remediation. Furthermore, the distribution of e-mail alerts upon changes in the corporate network allows for fast response times.

The CSI provides organisations with improved responsiveness and protection, ensuring business continuity and minimising business damage.



### About Secunia

Secunia is the world-leading provider of vulnerability intelligence and vulnerability management tools for the corporate IT infrastructure.

We are an independent, unbiased provider of vulnerability alerts and advisories, free of all vendor ties. Secunia collects, evaluates, verifies, and analyses security information. This security information is available through our databases and distributed to our customers, segmented according to their specific business needs. We are a trusted and valued source of information, recognised by users, vendors, analysts, and press worldwide.

Our in-house security research team, consisting of experts specifically selected from hundreds of candidates worldwide for their unique competencies, performs the evaluation and analysis of the security information. This devotion to research and verification is what makes us stand out from the rest.

We listen to what our customers need - which is why each of our solutions has a unique market position:

- Secunia Vulnerability Management Series
- Secunia Binary Analysis
- Secunia Software Inspector Series

## Features of the Secunia CSI

### CSI results

The Secunia CSI does the following:

- Scans for installed applications, down to the specific version.
- Identifies the installation path of every application.
- Checks if the application has the latest security patches installed.
- Checks if the application is end-of-life and no longer supported by the vendor.
- Informs you what patched, insecure, and end-of-life applications are on your network.
- Provides guidance for remediation.

### Deployment and management

- An agent-less scan of your network can be performed right after acquiring the Secunia CSI. Only standard Windows networking services are required to allow access to hosts in your network.
- Agent-based deployment is more robust and flexible for segmented networks and for networks with hosts that can go off-line (such as work laptops). The agent runs silently in the background and can be used even behind a firewall.

### Software scans

- Scans are done by connecting directly to the Secunia database via a secure SSL connection
- Proxy server details can be configured into the Secunia CSI.

### Non-intrusive, risk-free vulnerability scanning

The CSI is more than just a vulnerability scanner. Traditional scanners often attempt to run proof-of-concept scripts against a system. This approach includes "penetration" tests, which are not entirely safe for the network and often produce inaccurate results. CSI by-passes the need for intrusive testing, because it identifies the vulnerable applications through looking at every relevant executable and library and checking these against the world's best vulnerability database: The Secunia advisory database.

### Secunia Corporate Software Inspector - the ultimate companion

The CSI takes information accuracy to a completely new level, keeping you up-to-date regarding vulnerabilities in installed applications. You save both time and resources when handling vulnerabilities, because the CSI instantly maps your IT infrastructure and provides you with guidance on remediation and upgrading.

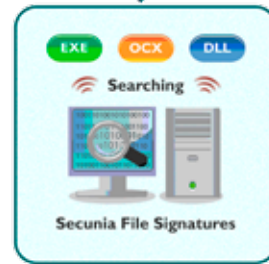
The CSI keeps track of all security issues, telling you what you need to know, when you want to know it, and how to remediate it, all in one go.

## Contact Secunia

Contact [sales@secunia.com](mailto:sales@secunia.com) for more information.



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



2 It scans all executables, including EXE, OCX, and DLL files using the Secunia File Signatures.



3 All scan results are fed into the central management console for easier analysis.



4 If an insecure application is identified, the Secunia CSI tells you which version to update to.

### How does it work?

Based on Secunia's world-class vulnerability intelligence, the CSI is capable of inspecting systems on the network and identifying installed programs down to the version number. This creates a highly accurate mapping of the installed applications and their versions. Using the Secunia advisory database, these mappings are checked for missing patches, giving you a complete overview of vulnerable software on the network.