Secunia
Stay Secure

Complete Patch Management

Targeted, Reliable and Cost-efficient

Secunia CSI

Corporate Software Inspector

Empower your organisation to take control of the vulnerability threat & optimize your IT-security investments

Secunia Corporate Software Inspector (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

- **Automatic identification** of vulnerabilities in your infrastructure (across endpoints and servers) grouped according to security status (insecure, End of Life) and criticality rating
- **Prioritised patching efforts** according to risk exposure, mitigation, and compliance standards
- **Optimized workflow** and remediation process through integration with patch deployment tools and automatic patch repackaging
- **Complete overview** of all programs, both Microsoft and non-Microsoft, installed
- **Patching of non-Microsoft programs** through existing patch deployment tools (for example WSUS, SCCM, Altiris)

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

Vulnerability and Patch Management are critical components of any security infrastructure because it enables **proactive detection and remediation** of vulnerabilities.

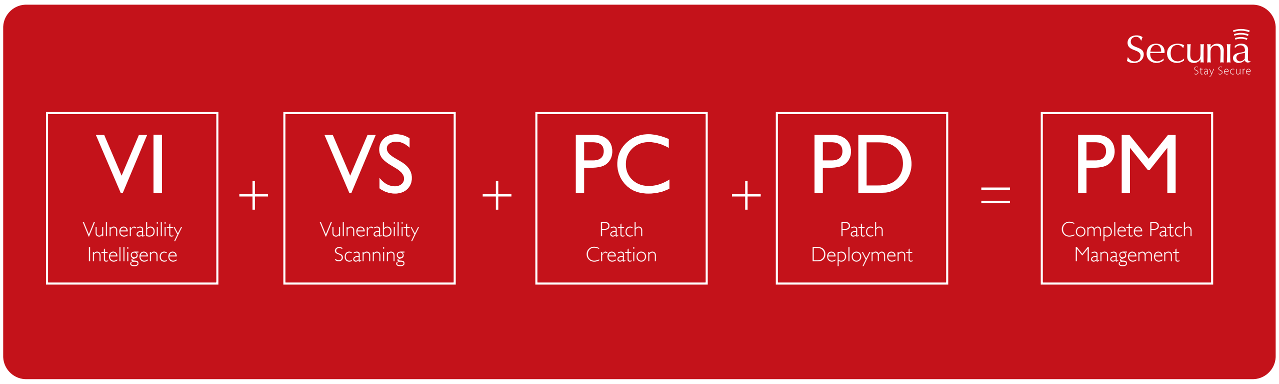
A process to identify vulnerable programs, including programs not authorised in a corporate environment, paired with targeted patch management is an absolute must to reduce the window of exposure and eliminate the root cause of a potential compromise. However, patching of vulnerable programs, in particular third-party programs which is not supported by Microsoft WSUS, has been a cumbersome and resource intensive process causing many enterprises to either neglect patching or only patch very few non-Microsoft programs.

This has left companies exposed as it only takes one vulnerability to compromise the security. This can lead to loss of end-user productivity, unplanned downtime, loss or exposure of sensitive data or damage to brand/reputation[1].

The Secunia CSI 6.0 is a Vulnerability and Patch Management Solution that completes the Patch Management process.

It provides organisations with a complete overview of their vulnerability threat landscape, identifies exactly where program vulnerabilities exist and guides on how best to prioritize and implement remediation efforts, all whilst leveraging and maximizing existing security investments in current Client Management (CM), Security Information & Event Management (SIEM), and Governance Risk & Compliance (GRC) tools.

The Secunia CSI provides the reliable, comprehensive, and up-to-date vulnerability intelligence and highly accurate scan results needed by IT-operations and security teams to effectively manage the threat posed by unpatched vulnerabilities.



[1] Aberdeen Group Research Brief: "Managing Vulnerabilities and Threats (No, Anti-Virus is not enough" 2010

What's in it for you?

Management

- Comply with regulatory standards (for example PCI-DSS or NERC-CIP) on patching of programs
- Utilise existing infrastructure to enforce security levels, i.e. SCCM integration for third-party patching
- Enable policy enforcement and document your compliance efforts in case of a breach
- Validated intelligence provided by independent 3rd party vendor (Secunia)

Operations

- Overview of installed programs' security state across endpoints and servers
- Scan and patch non-Microsoft programs cross-platform
- Automatic package creation by Secunia Research
- Prioritise patching efforts according to criticality of vulnerability based on Secunia VI
- Access to out-of-the-box patches

Security

- Secure off-site assets
- Cross-platform scanning
- Pinpointing the exact vulnerabilities affecting the network
- Providing in-depth details about vulnerabilities
- Audit, enforce, and document patching levels
- Verify security levels across MS, non-MS, and own (custom) program

Feature Highlights

Coverage

- Scan and assess the security state of practically all legitimate programs running on Microsoft Windows platforms
- Support for scanning of Windows, Apple Mac OSX, and Red Hat Enterprise Linux (RHEL) platforms
- Scan custom programs (non-public)
- Sources the Secunia Vulnerability Intelligence Database that covers all off-the shelf programs

Overview

- Apply SmartGroups to prioritize remediation efforts, as well as filter and segment data to enforce compliance
- Exact mapping of infrastructure and users to ensure the environment is in sync

Integration

- Manage and publish packages using third party patch deployment solutions such as Microsoft WSUS/SCCM or Altiris
- Active Directory (AD) changes can be automatically updated in the Secunia CSI
- Source SCCM for inventory and avoid installing agents and configuring the Secunia CSI
- Integration with the Secunia Vulnerability Intelligence Manager (VIM) to automatically create and update asset lists based on the Secunia CSI scan result
- PSI 3.0 Integration for management of decentralized endpoints

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.

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

Visit us at **secunia.com**