Secunia Personal Software Inspector

- Patching made easy -

Secunia PSI 2.0 - Setup and Usage Guide

Ver 1.0.0.2

Table of Contents

1. Secunia PSI 2.0 – Vulnerabilities and "patching"

The Secunia PSI is a vulnerability and patch scanner for your personal computer. It is a free tool designed for the sole purpose of helping you secure your computer from vulnerabilities. This is done by updating the insecure program to a later version that fixes the vulnerability, a process also referred to as "patching".

Unlike the many general update checkers available that will offer you to install any version that is newer than the one you already have installed, the Secunia PSI only suggests an updated version if the version you curently have installed is affected by a known vulnerability that the vendor has fixed in a newer version. Newer does not necessarily mean more secure.

What are vulnerabilities?
A vulnerability is basically a programming error/flaw in a program which can be used by a hacker to perform actions, which have a security impact on your computer. These actions range from stealing sensitive information (like credit card numbers, passwords, personal documents etc.) to automatic installation of viruses, trojans, keyloggers and other types of malware.

Vulnerabilities can affect all applications installed on your computer, from the Operating System down to your email client, office application, instant messaging client, and so on.

Why is this a risk to you? When you browse the Internet, you use an "Internet browser", this may be Internet Explorer, Firefox, Chrome etc. All of these browsers have repeatedly been affected by vulnerabilities that have allowed hackers to do practically anything on your computer - all you had to do was to visit a website and it could take control of your computer. The same goes for many other applications on your computer - unless you keep them updated and patched.

How can you protect yourself from vulnerabilities?
You simply need to keep your programs "patched". The only real solution, to avoid becoming a victim of a hacker exploiting vulnerabilities, is to install the latest security updates that the vendor of the program has released. In other words, make sure that you always have the latest secure versions of the software that you have installed on your computer.

This is where the Secunia PSI steps in; it will scan your computer for installed programs and determine if any of the programs is affected by a vulnerability for which the vendor offers a newer and secure version. You are then offered a download directly from the vendors own website, so that you can easily run the installer and update the detected program to a secure version.

As new vulnerabilities are found regularly, it is important to scan for vulnerabilities regularly. If no scan has been performed for 7 days with the Secunia PSI installed, it will start automatically.

2. System Requirements

This is the current list of requirements that must be met for the Secunia PSI to function correctly.

Supported Operating Systems (32 & 64 bit):

- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP - Service Pack 3

Privileges

To install and run the Secunia PSI you will need administrative privileges.

Connectivity

Access to Secunia servers (encrypted) via SSL (https://psi.secunia.com:443/) and access to Microsoft Update servers, see also Software Requirements below

Software Requirements

The latest version of Microsoft Update. You can determine whether or not you are running the latest version of Microsoft Update by visiting update.microsoft.com. If you are able to check your system for missing updates through this tool, your system should function properly with the Secunia PSI.

Hardware Requirements:

There are as such no additional hardware requirements. If your computer can run any of the above mentioned Operating Systems, then the Personal Software Inspector should also be able to run.

3. Download and installation

To download the Secunia PSI please go to http://secunia.com/vulnerability_scanning/personal and click "DOWNLOAD NOW". You can either open and run the installer directly or download it to your PC and double-click on it.

To install the Secunia PSI with recommended settings, simply follow the instruction on the screen. You will need to read and agree to our License Agreement.

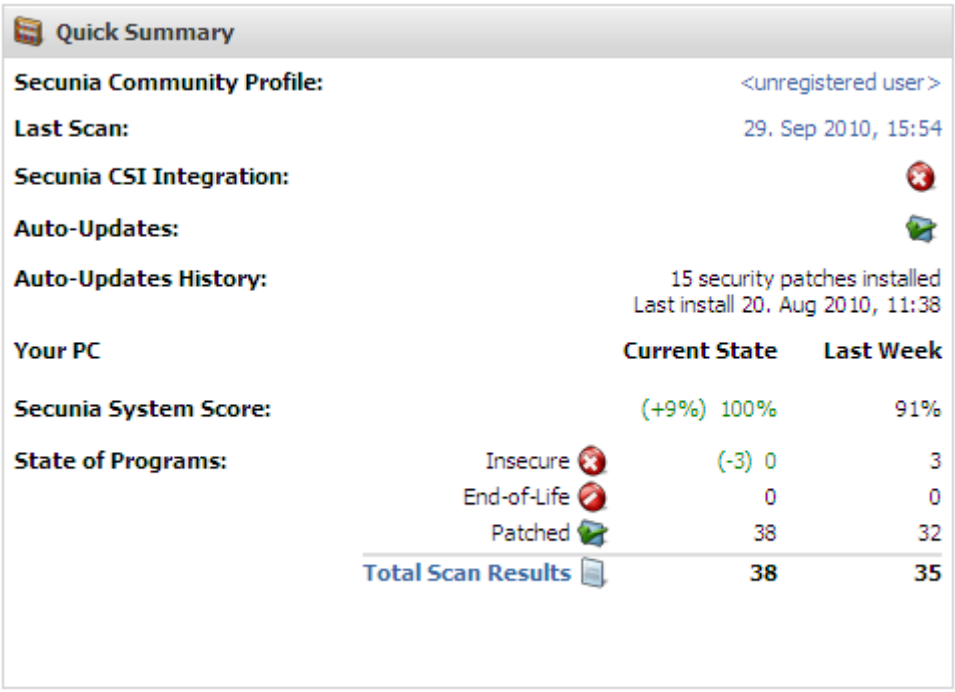
4. Using the Secunia PSI

This section goes through the tabs in the Secunia PSI and explains the features.

4.1 Dashboard

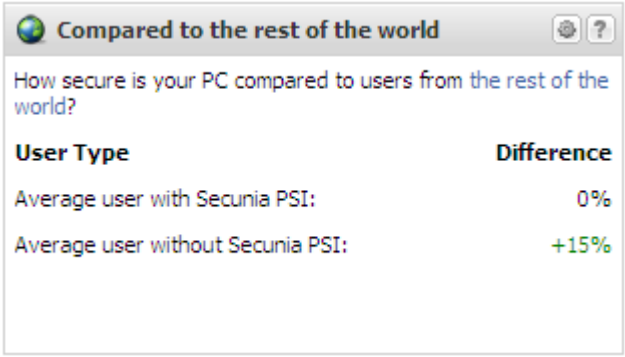
The Dashboard-tab presents an overview of the status of your computer, the historical development of your Secunia System Score, as well as a general comparison of your computer to the general security state of other computers with and without the Secunia PSI.

Quick Summary
This box shows a brief overview of your system. It will show if your instance of the Secunia PSI is tied to a Secunia community profile, the date and time of your last scan, whether or not Auto-Updates are globally enabled, as well as whether or not your Secunia PSI is integrated with a Secunia CSI installation (relevant only to corporate users).

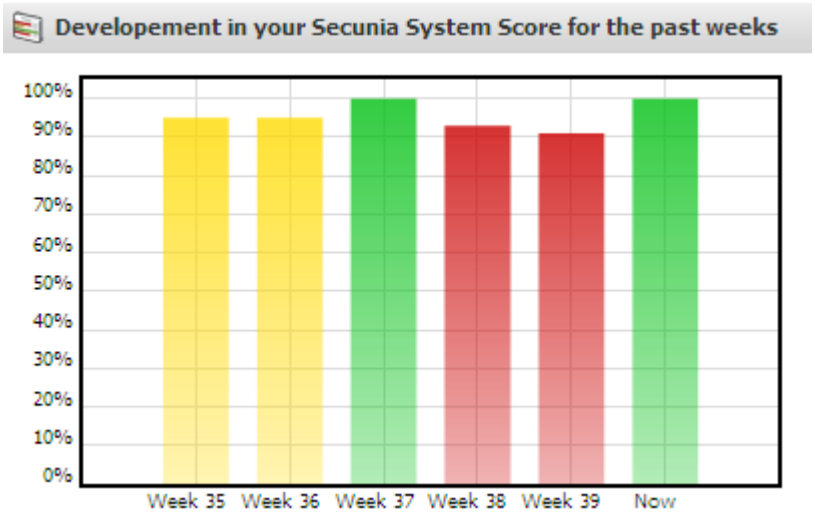


It will also show how many Secure, Insecure or End-Of-Life products you currently have installed, and how many there were last week.

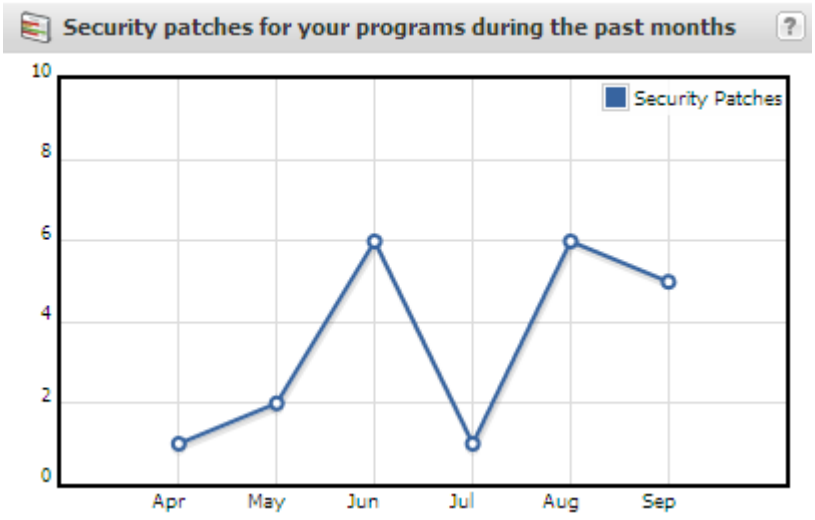
Compared to...
This box shows you a comparison of your current Secunia System Score and the average user, both with and without the Secunia PSI installed.



Secunia System Score
This graph shows the historical development of your Secunia System Score over the last 10 weeks. Green indicates a score of 100% while yellow and red indicates a score that is less secure.



Patch History
This graph shown the number of security patches that have been published for the programs you have installed on your PC. You can click the question mark for more information.



4.2 Scan Results

The columns explained

Clicking the "+" next to a program reveals additional information about the program, including its installation path and the exact detected version. There is also a button to create an Ignore Rule for the program that excludes it from future scans, and another for going directly to the folder where the program has been detected.

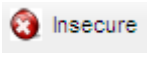
The Program-column shows you the name of the detected program along with its major version number.

The "#" column shows you the number of detected instances of the program. In most cases there will only be one. If there is more than one detected instance of a program, you can click the "+" to see the name and installation path of each instance.

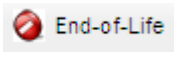
"Program State" shows you the state of each detected program as one of the following:

- **Patched** 

A program is considered as patched when all the latest security updates that are available from the vendor have been installed. Programs that are patched should as such not require any more attention from the user. Optimally all your programs should be in this category.

- **Insecure** 

Insecure means that the version installed have one or more known vulnerabilities which can be exploited by hackers and malware. It also means that the vendor of the program have released a "patch" that can solve the problem. To fix the problem you need to download and install the patch.

- **End-of-Life** 

This means that the program is no longer being maintained by the vendor. This means that when a vulnerability is found in the program, the vendor will not release any patch for it. Having such End-of-Life programs installed poses a potential security risk as you will not be advised about vulnerabilities and will not be able to update and patch them. It is recommended to either uninstall programs that are end-of-life, or update to a version that is still supported by the vendor.

When a program is detected as insecure, the "Threat Rating" column shows how severe the latest patched vulnerability is. There are 5 categories rating from "Not Critical" to "Extremely Critical". For a detailed explanation, please see the Secunia website: http://secunia.com/advisories/terminology/

The "Detected Version" column shows the exact version that the Secunia PSI has detected.

The "Install Solution" column should optimally read "Up-to-date" for all the listed programs (followed by a (AU) if the program can be auto-updated). If a program is Insecure or End-of-Life it will read "Install Solution". You can then click on "Install Solution" to download and install the secure version. Depending on the program this will work in one of two ways:

- Direct download: Whenever possible you will be given a download link from the vendors website that is direct. This saves the need to go to a website to choose the correct download.
- Download from website: When it is not possible to lead you to a direct download, your browser will open and go to the vendors website where you can download the latest version offered.

If a program installed on your computer has not been detected by the Secunia PSI, you can click the button "Are you missing a program?" in the upper right corner. This feature allows you to suggest programs that are currently not detected, so they can be added to the database. This will usually happen within 24 hours on weekdays.

Customising the columns
Using the "drag-and-drop" method it is possible to move and organise the columns. When the cursor is right above the top of a column, additional options show up that enables the user to sort the column as either ascending or descending. Each column can also be completely disabled to only show the information the user finds most relevant.

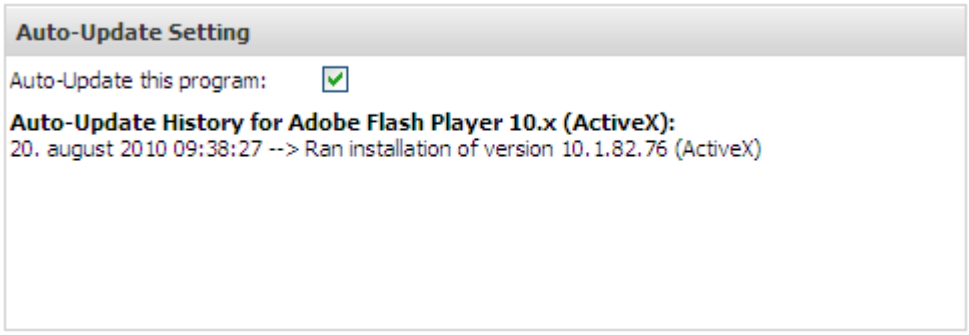
Note however that the column-settings will not be saved when closing the Secunia PSI, or reloading the interface.

Double-Clicking Program-Entries

For additional details about a detected program you can double-click it. That will bring up a Window with detailed information about the chosen program.

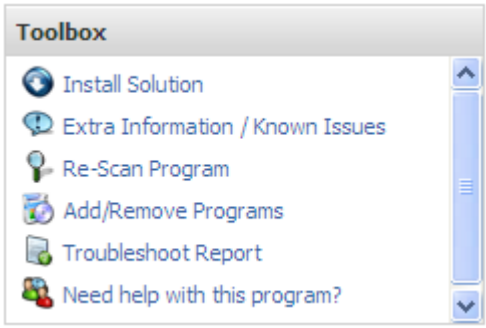
Quick Facts
This box will present the general security status of the program. A secure program will have a short message here, stating that the program is up to date, while an insecure program will show a warning in red, as well as the current and secure versions of the program.

Auto-Update Setting
This setting allows you to enable or disable auto-updates for one specific program (if the program is auto-updatable). Note however that auto-updates must be enabled in the Settings-tab for this to take effect.



Toolbox

The Toolbox gives you quick access to several useful tools for updating programs, and debugging any potential problem.



The "Install Solution" button will open the patch for the Insecure program in your default browser, or in Internet Explorer for programs that rely on Microsoft Update (the absolute majority of Microsoft programs).

"Extra information / Known issues" informs of any common problems with updating the program, maintained by Secunia to make patching as painless as possible. This option only shows up when available.

"Re-Scan Program" will run a limited rescan of just the selected program.

The "Add/Remove Programs" shortcut leads you to the build-in Windows Add/Remove Programs tool usually found in the control panel.

The "Troubleshoot Report" button presents a brief report with the details of the selected program. When seeking help on the Secunia Community Forum, including this report can help both the user experiencing difficulties, the forum regulars, and the Secunia support staff to reach a solution faster.

The "Need help with this program?" shortcut leads directly to the Secunia Community Forum, with recent threads about the selected programs pre-selected.

Online References
The "Online References" box gives the user quick access to in-depth information about the vulnerability in the selected program.

The "Secunia Advisory" button will take you directly to the Secunia Advisory for the vulnerability.

"Secunia Product Page" leads to the programs product page at Secunia, where you will find all Secunia advisories for the product, as well as statistics and program-specific details.

The "Vendor Product Page" button leads to the programs home on the vendor's website.

The "Problems / Discussions" shortcut leads directly to the Secunia Community Forum, with recent threads about the selected program pre-selected.

Detected Installations, right-click for further options

This field lists all installations of the program on your computer, including old versions that have not been successfully removed after updating or uninstalling.
Upon right-clicking any of the paths listed in this interface, you will be presented with a pop-up box that will offer you two choices: Open folder and Ignore Program.

Open folder simply takes you to the location of the detected file.

Ignore Program will exclude this program from future scans, as well as ensure it will no longer be present in your interface. Ignore rules, by default, ignores the entire folder in which the detected file is located.

4.3 Secure Browsing

This feature is only recommended for advanced users and will only be available if selected during the installation, or later enabled in the Settings-tab.

This tab will show you each of your installed browsers, its plugins, and whether any of these contain any known vulnerabilities. It is important to note that you will be alerted to vulnerabilities even if the vendor has not yet released a patch. Therefore you may see vulnerabilities that currently cannot be patched.

The purpose of the Secure Browsing-tab is to give the user the option to assess the current security of the installed browser(s) and its plugins. This enables the advanced user with several browsers installed to avoid the browsers with unpatched vulnerabilities, uninstall unpatched plugins, perform workarounds etc.

Please see the explanation in the Secure Browsing-tab itself for further details.

4.4 Scan

During scans the Secunia PSI starts by downloading the latest search rules from the Secunia servers so that the results will always be up-to-date. Then it searches for program files on all available drives and looks at the file version information. It then collects information about the operating system and uses Microsoft Update to determine if any Microsoft security patches are needed. Finally it sends all the collected program information to the Secunia servers where the programs are divided into 3 categories: Patched, insecure, and end-of-life. The results are then returned to the user and shown in the Secunia PSI.

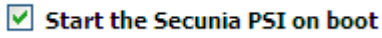
Any programs that show up as end-of-life or insecure pose a potential risk to your system, and will require further attention.

Please note that all information exchanged between the user and the Secunia servers are standardized and completely non-personal. None of the information can be used to identify a user, and an encrypted SSL-connection is used to prevent any third parties from snooping on the connection to the Secunia servers.

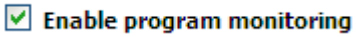
4.5 Settings

This tab contains the general settings that regulate the behaviour of the Secunia PSI.

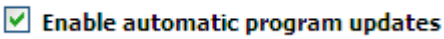
PSI Settings



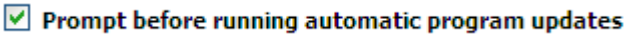
The "Start Secunia PSI on boot" check-box regulates whether or not to start the Secunia PSI immediately after Windows has started.



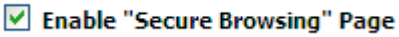
When "Enable program monitoring" is checked, the Secunia PSI will attempt to detect changes to the programs it monitors in real-time, notifying you if, for example, an Insecure program has been successfully patched, or entirely removed.



The "Enable automatic program updates" check-box determines whether the Secunia PSI should make use of its capability for automatic updates. When checked, it will attempt to automatically update any program for which this is possible, without requiring any user intervention. When not checked, programs have to be upgraded manually.
If there is a particular program you prefer not to auto-update, you can go to the Results-tab and double-click the program. Remove the check at the Auto-Update checkbox, and the program will no longer be automatically updated.



With this option enabled you will have to manually accept each automatic update before it can be performed.



Checking this option will add the tab “Secure Browsing” to the interface of the Secunia PSI. This tab will inform you of vulnerabilities in your browser and its extensions even before the vendor have released a patch that fixes it. This option is only recommended for advanced users.

Ignore Rules

Ignore rules are rules that specify locations the Secunia PSI will not scan or gather results from. These locations could include backup folders, music collections, or other locations where scanning with the Secunia PSI serves no useful purpose. If this rule is applied for a directory it counts recursively, meaning that no files in the ignored directory will be scanned or shown in the scanning results.

The button “Create Ignore Rule” allows you to actually create an ignore rule. The field "Rule Name" is simply a name, and what you choose to enter here has no impact on the scan results. The "Rule Path" field however, specifies the directory or folder to be ignored.
It must be entered in this format: "[DriveLetter]:\path\to\ignore".
Example: "C:\Documents and Settings\Music"

Drives

Here the Secunia PSI will list all detected drives on your system. Only your system partition (usually the C: drive), and the drive containing the "Program Files" directory (if this drive is different from your system partition) will be selected to be scanned by default.

The Secunia PSI will only scan the selected drives. Selecting a drive with a very large amount of files can significantly slow down the scan.

4.6 Secunia Community Profile

Create a new or update an existing Secunia Community Profile. Having a Secunia Community Profile allows you to participate in upcoming events, manage your Secunia mailing list subscriptions, participate in forum discussions, access more help, assist other Secunia PSI users, and get notified about new features from Secunia.
If you already have a Secunia Profile it can be recovered by entering the username and the email address associated to it.

4.7 Integrate with Secunia CSI

NOTE: This feature requires you to have a licence for, and successful installation of, the Secunia Corporate Software Inspector (CSI). Home users will not have any use for this feature.

As of version 2.0 of the Secunia PSI and version 4.1 of the Secunia CSI, it is now possible to create a link between your Secunia PSI and a Secunia CSI console. This enables the user of the Secunia CSI to follow how you patch as well as seeing the programs you have installed.

4.8 Support/Forum

The Secunia Community Forum
The Secunia Community Forum is the place where PSI users can discuss patching, product updates, exploits, the PSI, and anything else security-related.

We hope that you will create a Secunia Profile and join the discussions and help fellow PSI users achieve a perfect 100% Secunia System Score.

We generally invite, and recommend, all PSI users to open forum threads with their questions, recommendations, suggestions, and feedback. This way all PSI users can enjoy the vast amount of knowledge that will get collected here over time.

Updating And Patching
Patching programs isn't always as easy as it should be. Many vendors focus solely on getting their programs to market and in the process of rushing their programs out, they neglect to implement proper functionality for updating their programs, when e.g. security problems are discovered.

It is important to note that the purpose of the Secunia PSI is to detect installed programs, and determine if security threats, posed by vulnerable programs, are present on your computer. The actual solutions to the security threats comes from the vendors of your programs.

When it comes to the patches delivered by the vendors of your programs, then there is not much the Secunia PSI can do to help - this is the sole responsibility of the vendors. Unfortunately, not all vendors live up to their responsibility and you may end up with various problems - we invite you to join our forum and get help from other users.

Got a Problem Patching a Program?
Chances are that if you experience a problem, someone may have solved or experienced it before you, and are ready to assist you with your problem.

Secunia staff is monitoring the forum and we are, as many of our users, happy to assist with answers and suggestions to your problems.

We generally recommend all users to ask questions directly in the forum. This enables all users to learn from the solutions you find.

You can visit the Community Forum here: http://secunia.com/community/forum/

4.9 Privacy Statement

Communication
All communication between your system (The Secunia PSI) and the Secunia servers (psi.secunia.com) is conducted via an encrypted connection (SSL). Effectively protecting against eavesdropping of the data and the results being exchanged with Secunia.

Data
All data sent to Secunia is treated as confidential.

The Personal Software Inspector collects unique text strings and data about executable files and installed applications on your system, including hostname and langroup. This data is analysed by the Secunia File Signature engine (psi.secunia.com) to determine the exact applications installed on your system. No other data is collected from your system.

This can in turn be used to provide you with a detailed report about the specific missing security related updates on your system.

The data sent to Secunia is non-personal data only. The data is generic, standardised, and originates from installed programs on your computer.

All data will be deleted automatically no later than 12 months after you terminate using the program or immediately after you cancel your registration.

Secunia will not share or sell specific data about individuals with any third parties. Only aggregate statistics which can't be related directly to any individuals will be published and shared with third parties.

5. About Secunia

Secunia is an independent, world-leading provider of Vulnerability Intelligence.

The vulnerability issue cannot be denied. Every home user, as well as corporation, faces the certain knowledge that vulnerabilities can and is being used, to compromise security. How can you protect your computer effectively against malware and hackers exploiting vulnerabilities? How can you make sure to always have installed all security-related patches/updates that are available for your installed programs?

Our aim is to give you the information and tools you need to keep your computer updated and secure with the latest "patches". This will help you stay secure and avoid attacks by malware and hackers on the internet. We only direct you to the patches/updates officially offered by the vendor of the software that you already have installed.

Secunia offers several services to help both businesses and home users stay secure. For the home user we offer the Secunia OSI and the Secunia PSI completely free of change. We also offer a Community where you can seek answers to any related questions you might have, as well as sharing your own experiences with patching/updating.

6. Contact

If you experience any issues with the Secunia PSI, we provide you with the following options.

- **FAQ:** http://secunia.com/vulnerability_scanning/personal/faq/
- **Community/Forum:** http://secunia.com/community/forum/

The FAQ provides you with a list of the most common issues and how to fix them.

The Community/Forum gives you the option to receive support and advice from both Secunia Officials and other users. You can also participate in the ongoing debates and share your own knowledge about vulnerabilities, patching, general IT-security etc.

If you have been unable to find a solution in the resources above, you can contact us at support@secunia.com.