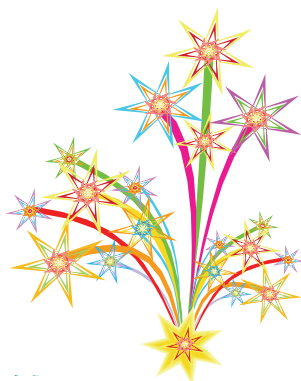




OTTAWA

Happy New Year!

PC NEWS

Volume 28, Number 1

January 2011

Product Review

Secunia PSI—Vulnerability management made easy *by Chris Taylor*

If you have been using computers since the 80's, you may remember a few things about software security vulnerabilities;

1. they were not often discovered by bad guys
2. they were infrequently patched by vendors
3. it was hard to find out that patches were available

Fast forward to the 90's.

Some vendors started showing concern over vulnerabilities, probably driven by the fact that the bad guys were getting much better and much faster at finding and exploiting security vulnerabilities. Microsoft was one of the most active in trying to make sure people patch their software (some might say they were the vendor that had the biggest need to patch for security vulnerabilities) and introduced Windows Update back in the late 90's. Although a little crude in the beginning, it worked and made it a lot easier to keep Windows patched.

Microsoft has continued to improve Windows Update over the years. Overall, it has become an easy and reliable way of keeping Windows and some other Microsoft software up-to-date. And it seems lots of people agree. According to Wikipedia, the Windows Update web site processes an average of 90,000 page requests per second and on Patch Tuesday, outbound traffic can exceed 500 gigabits per second.

But what of other vendors? Well, most have a much spottier record on making patches easy for the end user. Only in recent years have most of the big names built automated updating into their products. Adobe did not enable automatic updating in Adobe Reader until the spring of 2010. For a single purpose program, Adobe Reader has had an astonishing number of security vulnerabilities over the years. And don't get me started on security issues with Adobe Flash.

But even Adobe is now light years ahead of most vendors, most of whom simply have no way of automatically updating their software, leaving it to the end user to somehow find out if there are security vulnerabilities for which the vendor has written a patch.

Fast forward to 2010

The world of security vulnerabilities has become astoundingly chaotic. In October, Microsoft had a record 49 vulnerabilities fixed on patch Tuesday. Adobe Reader has been patched 6 times this year, always for multiple vulnerabilities. Apple, who likes to pretend they don't have security problems, patched iTunes 4 times so far this year, for a total of 63 vulnerabilities!

The bad guys are getting very good at quickly exploiting vulnerabilities. They reverse engineer patches to find how to exploit those who have not patched. There are zero-day exploits coming out that have no patch available, leaving vendors to (sometimes) scramble to get a

patch out. It is the wild, wild west out there, folks.

Secunia to the rescue

Secunia is a security firm founded in 2002 that focuses on vulnerability intelligence and management, tracking information about security vulnerabilities. And then they did a very nice thing for the health of the Internet and all the Windows computers attached to it; they released a wonderful program – free for home use – that keeps the software on your computer patched!

Secunia Personal Software Inspector (PSI) is a small agent that you install on your computer. I installed the 2.0 beta version. It scans your computer and collects version information embedded in all your program executables, dynamic link libraries, web browser plug-ins, etc. It then correlates this information with Secunia's product database and compiles a list of your installed programs. It then correlates this list with Secunia's vulnerability database to determine if any of your programs have security vulner-

(Continued on page 6)

Inside this issue:

<i>Calendar / Coming Up / Raffle</i>	2
<i>Review: Secunia PSI</i>	1,6,7
<i>Members' Favourites—Dec. 2010</i>	3
<i>Review: Exploring Linux—Part 16</i>	4,5
<i>Contact Information</i>	8

Next Meeting: **WEDNESDAY, January 12th, 2010**

January Raffle

Thanks to the generosity of Corel, we will be raffling off a copy of **Corel VideoStudio Pro X2**. Valued at \$100, this all-in-one video-editing software can help you in creating high-quality HD and standard-definition movies, slide shows and DVDs. Edit video or photos quickly and easily using the Movie Wizard, or take full control with hands-on creative tools. Even paint, write or draw on your video. Burn your movies on DVDs, or high-definition AVCHD and Blu-ray discs. Share on PSP, iPod or iPhone, or upload directly to YouTube. Watch your movies on set-top players or with the included Corel WinDVD program.

Tickets are, as always, a good deal at \$1 for one, a great deal at \$2 for three or the unbelievable bargain of \$5 for ten!

Coming Up...

► January 12, 2011

Clicking, Flicking and Tweeting: Social Networking Controversy.

The explosion of social networking websites such as Flickr, Facebook, blogging sites and Twitter has raised more than privacy concerns.

Join the discussion with Chris Taylor and Andrea Wells. Andrea will describe the value of social media sites, while Chris will give the cautions about using these tools so that you don't compromise your computer, your job, your identity, or worse.

November Prize Winners

George Leir was the winner of our door prize - a copy of the Quick Shadow software while **Harold McClemens** took home the raffle prize and is now the proud owner of a copy of Windows 7.

Congratulations to the winners and many thanks to QuicklyTech (<http://quicklytech.com/>) for providing a registered copy of QuickShadow Backup as the door prize for this meeting.

2010 CALENDAR

Meetings	Date	Time and Venue
OPCUG General Meeting	Wednesday, January 12 th	7:30 p.m. Auditorium of the Canada Museum of Science and Technology , 1867 St. Laurent Blvd. http://www.science-tech.nmstc.ca/english/index.cfm
Beginners' SIG	Wednesday, January 12 th	Immediately following the OPCUG General Meeting.
Linux / Open Source SIG	Wednesday, January 12 th	Immediately following the OPCUG General Meeting.
Beer BOF (Wing SIG East)	Wednesday, January 12 th	10:00 p.m. (after all other SIGs) at Liam Maguire's, St. Laurent Blvd. at Innes Rd.

Please note that unless otherwise noted, SIGs meet at 9:00 p.m. (immediately following the OPCUG General Meeting).

Members' Favourites – December, 2010 by Alan German

Scrooge came early to visit with members of the Ottawa PC Users' Group or, at least, his most well-known trait of not spending any (much) money was fully in evidence at our December meeting. The evening was devoted to "members' favourites". Four members of the group talked about their selections, all of which turned out to be software and/or hardware products that were either free or available at very low cost.

First up was OPCUG's President, Chris Taylor, exhorting us once again to keep our system security up to date, this time through the use of Secunia Personal Software Inspector (PSI). Secunia PSI is a free download that will scan the applications installed on your system for insecurities, and provide the ability to download patches to bring the software up to date. Chris demonstrated this on his netbook, over a live Internet connection, and downloaded one of the offered solutions to show how easy it is to identify and fix issues with outdated software. PSI will scan your system once a week in the background. It can be set to automatically update programs, or you can have the program notify you of available security updates. The only caveats are that (a) sometimes PSI's "Install solution" button doesn't work so that it may be necessary to go to a vendor's web site to obtain the updated software, and (b) any software identified as being an "end of life" version also needs to be manually updated.

Next, Jeff Dubois gave an interesting presentation entitled "Understanding VOIP". Jeff noted that, initially, he had found a cheap (\$3.95/month) provider of long-distance telephone service through World-line.ca, followed up with dial-up Internet access for his cottage through an associated company, 295.ca (\$2.95/month). These were the start of a quest to minimise his telecommunications' charges with a free phone line, software supplied by freephone-line.ca, the microphone and speakers attached to his computer, an analogue telephone adapter (ATA) – a \$50.00 hardware device – and a wireless (Bluetooth) telephone system (base station and handsets).

Alan German talked about some of the software products that had been included in past

and present issues of OPCUG's Free Software Guide, and some of the programs that will be included in the future. Past offerings included the free update checker from FileHippo.com that identifies and supplies new versions of any installed applications; Deskhedron providing the ability to place multiple desktops on a rotating cube; and Visipics, a utility that tracks down duplicate image files, even if the pictures have different resolutions or file formats (e.g. JPG or PNG). Sumatra PDF Reader, a replacement for Adobe Reader, and Process Monitor, a utility to positively identify processes running under the operating system, were two of the utilities featured in the most recent guide. Future issues of the guide are to include some interesting and useful software such as CombineZP, a utility to merge photographs in order to extend the depth of field; the web-based Geni family-tree system; HDClone, a disk imaging utility; QuickShadow, a real-time file backup system; two Canadian tax programs – Taxman and Studio Tax – and LAlarm, a software theft alarm for laptops.

The final presenter was Harald Freise with his selection of "Perhaps Useful Stuff" – starting with an endorsement for the utility, portability, and affordability of the netbook computer – and suggesting consideration of a large-screen, LED television for use as a computer monitor. Harald was also enthusiastic about VOIP, mentioning Skype (and Google Voice) as a viable method for making long-distance telephone calls for \$28/year anywhere in North America. For on-line music, Harald suggested using Radio? Sure! to access more than 200 thousand radio stations around the world. Songr, a web-based search engine, provides a means of identifying and locating a specific tune based on a snippet of its lyric – as evidenced by Harald tracking down a YouTube video of a weird and wonderful big band number involving bananas! Picasa and the associated Picnik editor were suggested for digital image management and modification, while the final utility mentioned was Ultradefrag, a fast and efficient disk defragmenter and optimizer.

Bottom Line

Secunia Personal Software Inspector (Chris Taylor)

http://secunia.com/vulnerability_scanning/personal/

Copies of the noted presentations may be downloaded by OPCUG members from File Area 43 – Presentations – on The PUB as follows:

Understanding VOIP (Jeff Dubois)

<http://opcug.ca/code/html-fdnld?frames=n&recno=5162496>

OPCUG's Free Software Guide – Past, Present, and Future (Alan German)

<http://opcug.ca/code/html-fdnld?frames=n&recno=5163776>

PUS (perhaps useable stuff) (Harald Freise)

<http://opcug.ca/code/html-fdnld?frames=n&recno=5165056>

And, how could you not check out:

Loving You Has Made Me Bananas (Guy Marks)

<http://www.youtube.com/watch?v=dh5oaxyMt0I>

Product Review

Exploring Linux—Part 16

by Alan German

OPCUG members will be well aware of my penchant for all things backup, and will likely have noted my recent discovery of QuickShadow, a Windows' utility, that offers real-time file backup from a source to a target disk drive. Having found this to be a really useful package for continually backing up all of my data files when working in Windows, I turned my mind to see if the same sort of functionality was available in the Linux world. After all, why should Windows' users have all the fun?

My web searches initially located two sorts of products. Firstly, there was a motley assortment of unfinished, and seemingly-abandoned, open-source applications that did not look at all promising. Secondly, there were several server-based solutions that appeared to be overly complicated to implement. However, I persevered, using several different search terms, and scanning a number of different web sites, until I came across a reference to the “inotify” feature that is present in recent Linux kernels. Inotify monitors disk activity and, in particular, flags when files are written to disk or deleted. A little more searching located a package that combines inotify's file event monitoring with the rsync file synchronization utility in order to provide the real-time file backup capability that I was seeking.

The software, named inosync, is actually a Python script, effectively provided as open-source code, by the author, Benedikt Böhm from Germany (<http://bb.xnull.de/>).

The bad news was that I had absolutely no knowledge of the Python scripting language. The good news was that Benedikt had provided a set of files that, with just a little simple tweaking, could be customized for any end-user's system. Furthermore, not only is inosync available in Ubuntu's software repositories, and so can be downloaded and installed from the Ubuntu Software Centre, recent versions of Ubuntu come with Python pre-installed so that the scripts can be used immediately.

The main script file is inosync itself (inosync.py), located in the /usr/bin/ file folder; however, there is usually no need to modify this file. Normal customization of the program is handled through a second script file, the example for which is given as sample_config.py. The minimum changes that need to be made to this latter file are to specify the disk or file folder to be monitored as the source of any file updates, and the disk or file folder to be used as the target where the backup is to be maintained. In my case, I changed the script file name to inosync_config.py and modified two lines in the

source code to specify my source and target disks as:

```
# directory that should be watched for changes
wpath = "/media/Data_Disk/"
```

```
# common remote path
rpath = "/media/USB DATADISK/D/"
```

Lines beginning with the # character are comments. The wpath variable specifies the data partition of my hard drive as the file source, and the rpath variable specifies an external USB drive as the target for the backup. (The /D folder on this latter disk is used for compatibility with QuickShadow in Windows that stores its backup to the same USB drive, but insists on locating the file directory in the “D” folder since Data_Disk is actually Drive D: under Windows.)

The command line to call inosync, and initiate the backup process is:

```
inosync -c ./inosync/inosync_config.py -d -v
```

where the c switch indicates the name and location of the configuration file to be used, the d switch tells inosync to “daemonize” (i.e. run in the background), and the v switch causes debugging information to be printed as necessary.

Now, I find that this command is way too intricate to be entered manually, so I use a simple bash script file instead.

```
#!/bin/bash
echo "Mirror DataDisk to 4GB USB"
# Check that Data_Disk is mounted
if grep '/media/Data_Disk' /etc/mtab > /dev/null 2>&1; then
    # Check that the 4GB USB memory stick is available
    if grep '/media/USB DATADISK' /etc/mtab > /dev/null 2>&1;
    then
        inosync -c ./inosync/inosync_config.py -d -v
    else
        echo " "
        echo "Insert the 4GB USB memory stick and try again"
```

(Continued on page 5)

Exploring Linux—Part 16 *(Continued from page 4)*

```

    echo " "
fi
else
    echo " "
    echo "Mount Data_Disk and try again"
    echo " "
fi
echo "Shell command complete"
read

```

The above file checks that the data partition is mounted, and that the USB drive is inserted into a port, before it calls `inotifywait` and sets the backup in progress. If one of the two disks is unavailable, the script issues an error message and quits. Otherwise, the script completes and `inotifywait` runs in the background, silently copying any new or updated files that are written to the source drive onto the target disk, and deleting from the target any files that are removed from the source, all while maintaining the source disk's directory structure.

As indicated, the “silent” backup process would normally be relatively transparent to the user. However, it is fascinating to open a Nautilus window to the source disk, and a second instance of Nautilus for the backup drive, and watch in more-or-less real time as changes on the source are reflected on the target drive. Files appear – or disappear – in the second window as if by magic! But, don't be concerned if the changes you make are not shown immediately on startup. Depending on how big your source disk/folder/files are, `rsync` requires some time to conduct the initial file synchronization. But, once this is done, changes are shown in mere seconds (and the time delay is one of the options that can be configured).

The program's documentation is not very extensive (perhaps not surprising given that the main Python script is just two pages of code) but is adequate for the task. However, a little further tweaking of the exemplar code is sometimes necessary. For example, since I was initially unaware of the time required for `rsync` to first synchronize the two drives, I was concerned that the program seemed to be hung because the changes I was making didn't seem to be reflected in the target window. In consequence, I tried to setup a log file to see what was actually happening. Using the format shown in the exemplar configuration file, I modified the entry `logfile = /var/log/inotifywait.log` to `logfile = /home/toaster/inotifywait.log`, hoping to create a log file in my machine's home folder; however, I couldn't get this to work until I placed the file name in quotes as `logfile = "/home/toaster/inotifywait.log"`. As I indicated earlier, I don't know anything about Python scripting, but I suspect that the above is an oversight in the documentation since, as noted earlier, the

`wpath` and `rpath` variables both use quotes for the file names.

But, to be fair to the program's author, he is very accessible (by E-mail), and more than willing to fix things, as I found out when I ran across another issue while trying to configure file exclusions. The configuration file has an “exclude list for `rsync`” that essentially lets you specify files that are to be excluded from the synchronization process. I wanted to have two files excluded, both of which were hidden SyncToy database files, one on the source disk and the other on the target drive. These files are used by Microsoft's SyncToy file synchronization program to determine which modified files and folders need to be processed. Each file is named `SyncToy{long_text_string}.dat` where the text strings are different for the two files. Now these files pose a problem to file mirroring software in regular operation. The file on the source disk does not exist on the target drive so it is copied to the target. Similarly, the original database file on the target disk is not present on the source drive so it is deleted from the target! The result is that the two SyncToy database files are now identical on the two disks and SyncToy chokes when it is run.

Since I wanted to use SyncToy to verify that `inotifywait` was working correctly, I needed the two files to be excluded from the mirroring exercise. However, although I specified the two files correctly in the configuration file, the SyncToy file on the target was always replaced by the file from the source when `inotifywait` was initiated. I found a work-around for this problem by hard-coding the two excludes in the main `inotifywait.py` file. But, I also sent an E-mail to Benedikt asking what I was doing wrong (remember – I don't really know how to code in Python!). The reply arrived the next day – there was a typographical error in the original code that was preventing the script from executing the exclude command properly. Furthermore, he provided a link for me to download a brand-new release (Version 0,2,3) of the package – coded that day – that fixed the problem. Now, that's service!

So, now I have the best of both worlds. When running Windows, I use QuickShadow to keep a complete backup of my hard disk data partition on my USB drive and, when running Linux (which is more usual), `inotifywait` maintains the backup of the same data files to the same USB drive. A marriage made in heaven! Thanks Benedikt!

Bottom Line

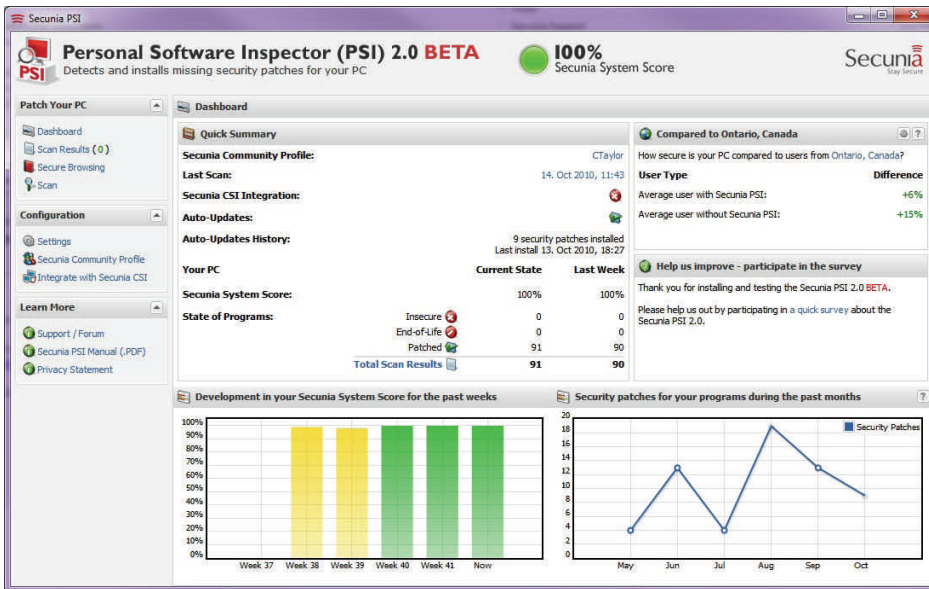
`inotifywait` (Open Source)

Benedikt Böhm

<http://github.com/hollow/inotifywait>

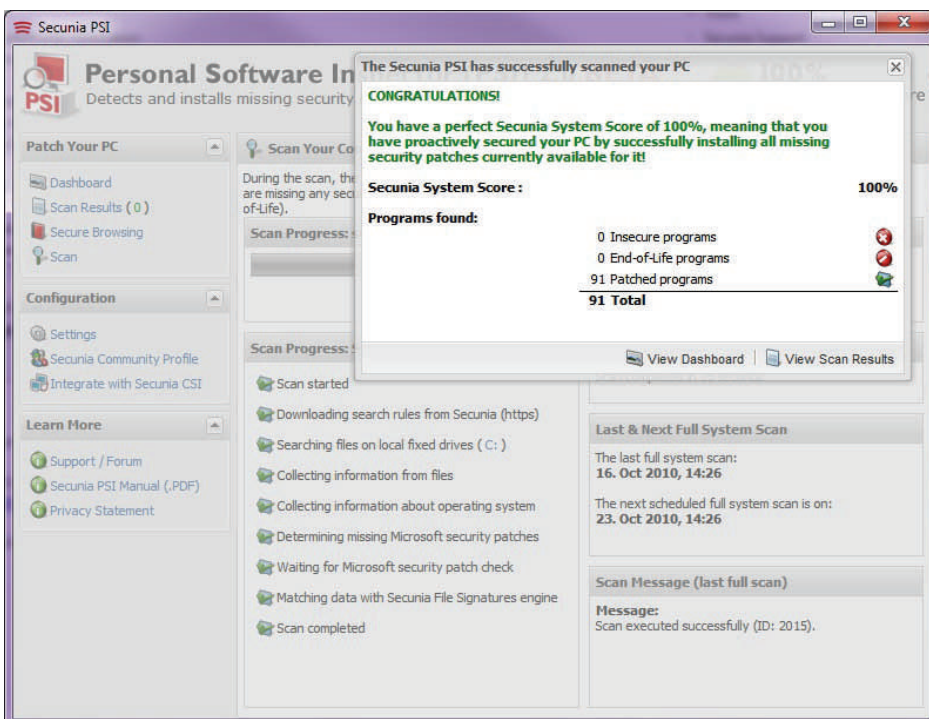
Secunia PSI... (Continued from page 1)

abilities and, if so, if there are patches available to address the vulnerabilities.



Once the scan finishes, which only takes a few minutes, all your installed programs are listed and insecure programs are highlighted in red at the top of the list. Secunia includes a vulnerability rating so you can know how severe the problem is. Right from that screen, you can view more details about the program. If it needs a patch, you can initiate it right from a link.

There are some programs that Secunia cannot patch by itself for some reason. In those instances, you will get a link to the vendor's site so you can deal with the problem manually.



By default, PSI will automatically scan your computer once a week looking for new programs or new vulnerabilities. The tray icon will change from a re-assuring green to yellow or red if vulnerabilities are discovered.

PSI has a fair amount of configurability, depending on how automatic you want things to be. You can go from totally manual, where you have to load the program and initiate scans and manually approve patches, right up to having it load automatically, monitor when new programs are installed or removed, and download and install patches automatically as PSI sees they are required.

I have opted for almost the most automatic configuration of PSI. The only non-automatic choice I made was to have PSI prompt for approval to apply the required patches. The reason I do this is not because I want to refuse a security patch. I always accept security patches. But I am curious as to how often I am getting patches and this will let me keep better tabs on things.

Proof in the pudding

As many of you know, I am a little paranoid when it comes to the security of my computers. I work in IT security. I give presentations at the Ottawa Public Library on how to protect your computer. So, when I first installed PSI, I thought it would give me the added assurance that I am up-to-date on all my security patches. Imagine my surprise when it told me 2 of my 90 programs had security vulnerabilities for which patches were available.

One was Infanview – a really nice, free, image viewer. I never thought to check if Infanview had security vulnerabilities.

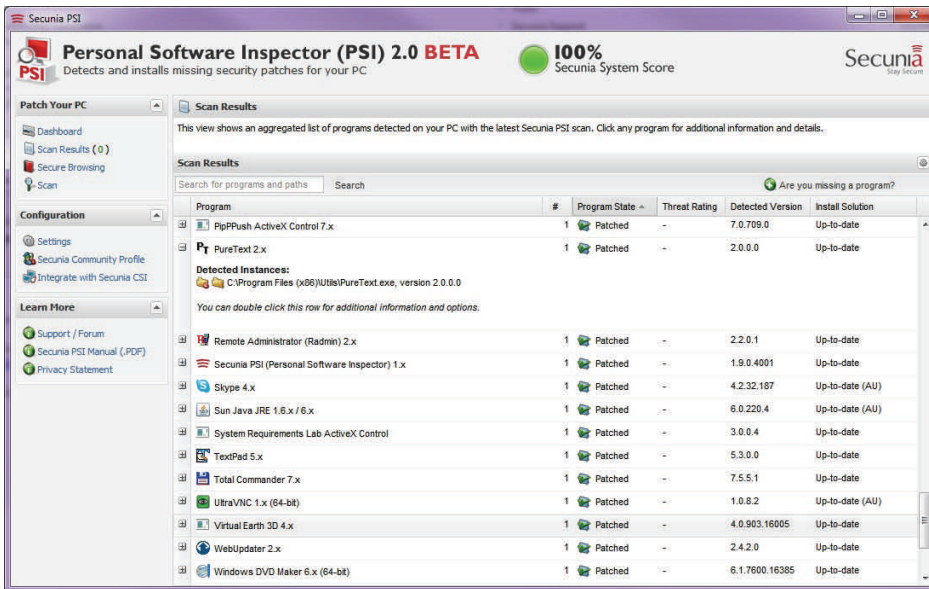
The second was an open source component included in TubeSucker – a free program for downloading YouTube videos. I never would have found that one on my own.

So far, I have installed PSI on half a dozen computers of mine, friends and family. None of them have reported as

(Continued on page 7)

Secunia PSI... (Continued from page 6)

fully patched when PSI was installed.



What about unknown programs?

What if Secunia's database of over 12,000 programs does not cover some of yours? Well, if your program is so obscure that Secunia does not know about it, it is pretty unlikely the bad guys are looking for security vulnerabilities in it and actively writing exploits. But it could happen.

I noticed I have a program installed that is not on PSI's list of programs found on my computer; a nifty little program called FotoSketcher that can apply paint-like effects to your digital images. So, I clicked the link in PSI; "Are you missing a program?", and was walked through a process to submit info to Secunia so they could track it in the future. But I couldn't submit it. It turns out the author did not embed version information into the executable. Without version information, there is no way for Secunia to track for vulnerabilities.

PSI is an amazing program that every Windows user should install. Secunia is to be commended for making this tool available free for home use. Highly, highly, highly recommended!

Bottom line

Secunia Personal Software Inspector 2.0 beta

Free for home use

System requirements: Windows XP SP3, Vista, or 7 with the latest version of Microsoft Update

Both 32-bit and 64-bit Windows supported

http://secunia.com/vulnerability_scanning/personal/

OTTAWA PC NEWS

Ottawa PC News is the newsletter of the Ottawa PC Users' Group (OPCUG), and is published monthly except in July and August. The opinions expressed in this newsletter may not necessarily represent the views of the club or its members.

Member participation is encouraged. If you would like to contribute an article to Ottawa PC News, please submit it to the newsletter editor (contact info below). Deadline for submissions is three Sundays before the next General Meeting.

Group Meetings

OPCUG meets on the second Wednesday in the month, except July and August, at the Canada Museum of Science and Technology, 1867 St. Laurent Blvd, Ottawa. Meetings are 7:30–9:00 p.m. and Special Interest Groups (SIGs) go until 10 p.m.

OPCUG Membership Fees:	\$25 per year	
Mailing Address:	3 Thatcher St., Nepean, Ontario, K2G 1S6	
Web address:	http://opcug.ca	
Bulletin board — The PUB (BBS)	http://opcug.ca/default.htm	
 President and System Administrator		
Chris Taylor	chris.taylor@opcug.ca	613-727-5453
Meeting Coordinator		
Andrea Wells	andrea.wells@opcug.ca	
Treasurer		
Alan German	alan.german@opcug.ca	
Secretary		
Gail Eagen	gail.eagen@opcug.ca	
Membership Chairman		
Mark Cayer	mark.cayer@opcug.ca	613-823-0354
Newsletter		
Brigitte Lord (editor/layout)	brigitte.lord@opcug.ca	
(Mr.) Jocelyn Doire (e-mail distribution)	jocelyn.doire@opcug.ca	
Public Relations		
Morris Turpin	PR@opcug.ca	613-729-6955
Facilities		
Bob Walker		613-489-2084
Webmaster		
Brigitte Lord	opcug-webmaster2@opcug.ca	
Privacy Director		
Wayne Houston	privacy2@opcug.ca	
Special Events Coordinator		
Bob Gowan	bob.gowan@opcug.ca	
Beginners' SIG		
Chris Taylor	chris.taylor@opcug.ca	613-727-5453
Linux / Open-Source SIG		
Andrea Wells	andrea.wells@opcug.ca	

© OPCUG 2011.

Reprint permission is granted* to non-profit organizations, provided credit is given to the author and *The Ottawa PC News*. OPCUG requests a copy of the newsletter in which reprints appear.

*Permission is granted only for articles written by OPCUG members, and which are not copyrighted by the author.

How to get the OTTAWA PC NEWS by e-mail



Want to get the newsletter electronically? There are two formats available: plain text and Adobe Acrobat PDF. Simply send a message to **listserve@opcug.ca**. Leave the subject blank and in the body of the message, type:

subscribe newslettertxt
(to get the plain text version).

or:

subscribe newsletterpdf
(to get the Adobe Acrobat PDF version).

And if you decide you do not need the printed version mailed to you anymore, simply let Mark Cayer (membership chairman) know. He can be reached at general meetings, as well as by e-mail at **Mark.Cayer@opcug.ca**. You might want to wait until you have successfully received at least one issue electronically before opting out from the printed version.

To subscribe to the Announcements List, e-mail **listserve@opcug.ca**. Leave the subject blank and in the body of the message, type:

subscribe announcements

Within a couple of minutes you will receive a confirmation message from the listserver.

“Announcements” is a low volume list that the Board of Directors uses to get in touch with the membership. Subscribers can expect at least one message per month – the meeting reminder that goes out a few days in advance of the general meeting. Other than that, the only time it is used is when the Board feels there is some important news that should be brought to the attention of all members.