Secunia for ISU IT Staff: Secunia CSI Reporting and Updating at Iowa State University

Jeff Balvanz
ISU Information Technology Services

Secunia Corporate Software Inspector is a system that collects information about the third-party software installed on computers running Microsoft Windows, compares it to a database of known software vulnerabilities and generates reports. The information collected can then be used to update those computers either manually or using WSUS or SCCM. The CSI console can be used to download updates and place them into the corporate WSUS server, where they can be automatically downloaded and installed to the vulnerable computers as part of the regular Windows Update process.

CSI is really designed for a more centralized IT system than exists at Iowa State. The number of administrators that can access the console is limited. Software updates added to the system are automatically approved for installation on all computers. Reports for groups of machines can be generated on a schedule and mailed to an administrator, but the machines in the group must be selected by checking boxes in a list of all the machines in the system and the group cannot be edited, only deleted and re-entered. Needless to say, we often felt like we were driving a square peg into a round hole.

After some development time, we believe we have a system that will allow departmental IT staff to make use of CSI. You can:

- Install updates automatically on on-campus machines, whether the machine is connected to the IASTATE domain or not;
- Collect information about vulnerable third-party software on your computers, whether they are on the IASTATE domain or not.

Information about the software installed on your computers is gathered by the CSI Agent, a 668 KB application that can be either installed as a service, run as a scheduled job or run manually. It can either return the information to the Secunia server, where it can be compiled into a report on a group of machines, or it can create individual report files for each machine that can be collected or emailed automatically.

The ITS Secunia administrators use this information to create update packages for vulnerable software. These are placed on the ISU WSUS server, sus.iastate.edu. A machine can be configured to use that server as the Windows Update server; if the machine is placed in one of the Secunia-related client-side targeting groups, it will also receive updates to any vulnerable software installed as part of Windows Updates.

Before third-party updates can be applied, there is a security certificate that must be installed. If you wish to install it manually, it is available at \\software.iastate.edu\ccsg\Secunia\SecuniaWSUSCertificate.cer. Otherwise, it can be installed via group policy or via the CSI Agent installation package. For more information on manual installation, see Appendix A.

Installing CSIA via Group Policy

If a machine is attached to the IASTATE domain and you wish to use WSUS to apply third-party updates you can do the entire installation via Group Policy:

1. **Install the Secunia certificate.** Apply the Group Policy object "ISU WSUS-CSI". This object installs and enables the certificate and points the machine at the ISU WSUS server for updates.
2. **Select a Secunia-related client-side targeting group.** The three Secunia-related groups, along with pre-created Group Policy objects putting the machine in that group, are shown in the table below. Simply apply the appropriate GPO to your machines.

Targeting Group	Description	Group Policy Object
SCPlusSecunia	Receives Microsoft "Critical", "Security", "Service Packs", "Update Rollups" and "Definitions" updates, plus all third-party software updates	ISU WSUS-SCPlusSecunia
NoDriversPlusSecunia	Receives all Microsoft updates except hardware drivers, plus all third-party software updates	ISU WSUS-NoDriversPlusSecunia
AllPlusSecunia	Apply all Microsoft and third-party software updates	ISU WSUS-AllPlusSecunia

NOTE: unless you select one of the Secunia-related client-side targeting groups, using either one of these GPOs or some other method, the machine will not have the Secunia agent installed or receive any third-party software updates.

3. **Configure Automatic Updates for the machine.** GPOs beginning with "ISU AutoUpdate" are available; apply the existing one for the appropriate update time, or create your own GPO.

Once you've applied these policies, the CSI Agent will install the next time the machine runs Windows Update.

Installing CSIA via Installation Package

Machines on campus that are not attached to the IASTATE domain can still use the WSUS server for Windows Updates and can receive third-party updates via Secunia. ITS has prepared an installation package that installs the necessary certificate and adds the computer to one of the Secunia client-side targeting groups. The CSIA agent will then install at the next Windows Update check. The installation package is available at \\software.iastate.edu\ccsg\Secunia\SecuniaDeploymentPackage.zip. Once you've unpacked the zip archive, you can use this installation package in either of these two ways:

1. **Run the "InstallSecunia.cmd" file.** In Windows Vista or Windows 7, right-click the file and choose "Run as Administrator". In Windows XP, log in as an administrator and double-click the file. This will install the certificate and put the machine in the SCPlusSecunia targeting group. The CSI agent will be installed at the next Windows Update.
2. **Select a targeting group.** From a command prompt run as an administrator, change to the directory containing the installation files and type the following:

   ```
   InstallSecunia /targetinggroup groupname
   ```

   where "groupname" is one of the targeting group names above. The CSI agent will install itself at the next Windows Update.

   If you specify the full path to the "InstallSecunia" file, you need not change to the installation directory; the program will locate its supporting files when necessary.

Neither of these procedures configures Automatic Update; you'll have to use the Automatic Updates control panel or some other means to do that.

The installation package can also be used to remove the CSI Agent. From a command prompt run as an administrator, change to the directory containing the installation files and type the following:

```
    InstallSecunia /remove
```

Installing the CSIA Service Manually

If you want to use CSI for reporting purposes but do not wish to have updates installed automatically from the WSUS server, you can install the CSI Agent service manually. The CSI Agent software is available at \\software.iastate.edu\ccsg\Secunia. You can install the CSI Agent software in one of the following ways. Note that neither of these techniques will install the necessary certificates for installing third-party software updates; these work for reporting only.

Install Using CSIASetup.exe

Enter the following command:

```
\\software.iastate.edu\ccsg\Secunia\CSIASetup.exe
```

This install is silent; you won't see any window or confirmation. The CSI Agent will immediately begin reporting to the Secunia server.

Install Manually

1. Place csia.exe in a known location in the Windows path. (C:\Windows\system32 is fine.)

2. Start a command prompt (as an administrator if you're using Windows Vista, 7 and 8) and change to the directory containing csia.exe.
3. If you're using 32-bit Windows, type the following at a command prompt:

   ```
   regedit /s \\software.iastate.edu\ccsg\Secunia\ISUConfig.reg
   ```

   If you're using 64-bit Windows, type the following:

   ```
   regedit /s \\software.iastate.edu\ccsg\Secunia\ISUConfig64.reg
   ```

4. For all versions of Windows, type

   ```
   csia -i -L
   ```

The CSI Agent will immediately begin reporting to the Secunia server.

Removing the Agent Manually

To remove the agent service manually, start a command prompt as an administrator and enter

```
csia -r
```

Then delete csia.exe from wherever you placed it.

There are additional options on the csia command that can be used to specify the check-in interval, configure a proxy server, and set other options; see Appendix B for more details.

Including the CSI Agent on Machine Images

Unfortunately, you can't just include the CSI Agent on a machine image. Each CSI agent has a unique identifier that is created when the agent is installed. If you simply put the agent on an image, but never go through one of the installation steps above, all of your machines will report to Secunia as the computer that the image was created on. Be sure that you run the `csia -i -L` command on each machine as part of the deployment process. Installing the agent using Group Policy is probably the easiest approach.

Running the CSI Agent as a Scheduled Task

The CSI Agent is a small application. When installed as a service, it only requires 3,500K of memory. Nevertheless, you may not want to have it running all the time. If not, you can run the CSI Agent as a scheduled task. Using either the Scheduled Tasks control panel or the SCHTASKS command, create a scheduled task to execute this command line:

```
Csia -c -L
```

For more information on the SCHTASKS command see http://msdn.microsoft.com/en-us/library/bb736357(v=vs.85).aspx.

Collecting Information on an Individual machine

If you'd like an immediate report on the vulnerability status of an individual computer, the CSI agent can save its results as either a CSV or XML file. At a command prompt, type one of the following:

```
csia -c -L -oc filename.csv

Csia -c -L -ox filename.xml
```

(This assumes that csia.exe is in the Windows path; enter the complete path if necessary.) You can specify a full path for "filename" and save the files in a shared directory if you want. This command can also be run as a scheduled task.

ITS has created a PowerShell script that will run the CSI agent, save the results to a CSV file, and e-mail that file to an email address specified in the script. It is available at \\software.iastate.edu\ccsg\Secunia\SendIndividualCSIAReport.ps1. PowerShell 2.0 or higher is required. You will need to edit the script to insert the appropriate email addresses.

Applying to Receive Digested Information

You can receive weekly reports on the vulnerabilities of your machines from ITS. This is possible whether your machines are on the IASTATE domain or not, but the way you'll sign up to receive reports will differ. (If you have both types of machines you can request both types of report.)

On-Domain Machines

If you are an OU Administrator, you can get reports on all the machines in an OU that are running the CSI Agent. Send e-mail to Secunia-admins@iastate.edu with the following information:

1. Your name
2. Your department
3. Your email address
4. A list of the OUs for which you want reports.

You'll receive a separate CSV file in an email each week for each of the OUs you support.

Off-domain Machines

To receive reports for machines that are not on the IASTATE domain, send e-mail to Secunia-admins@iastate.edu with the following information:

1. Your name
2. Your department
3. Your email address
4. A list of the NetBIOS names of the off-domain machines for which you want reports.

You'll receive a single CSV file in an email each week covering all of the machines you support.

Interpreting the Reports

The report you'll receive will contain a comma-separated-variable file with eleven columns of data as follows:

1. Host – the NetBIOS name of the machine.
2. Netgroup – the domain or workgroup the machine is in. (It is possible to specify a different netgroup with an option on the CSIA.EXE command line; see Appendix B.)
3. Last Scan – the last time the machine contacted the Secunia server.
4. Program – the name of the program detected.
5. Version – version of the program.
6. State – one of the following possibilities:
    - **Insecure** – a current package, but has one or more vulnerabilities categorized by Secunia.
    - **End-of-life** – a package no longer supported by the manufacturer with one or more vulnerabilities. You should plan to replace these packages with current versions, especially if the criticality level is four or higher.
7. SAID – the Secunia Advisory number for the package, always in the form SA*nnnnn*. You can read the advisory by going to the URL http://secunia.com/advisories/*nnnnn.*
8. Criticality – a measure of the seriousness of the vulnerability, where 1 is "Not Critical" and 5 is "Extremely Critical". Level 5 indicates that the vulnerability can be exploited remotely over the network and that exploits have been seen in the wild and may already be attacking your machine. A definition of each level is available at http://secunia.com/community/advisories/terminology/.
9. SAIssued – the date the advisory was issued by Secunia.
10. Vulnerabilities – how many different vulnerabilities exist in the software.
11. Path – the location of the software on the machine's hard disk.

The columns are separated by commas and the file can be opened by many programs. In Excel 2007 you can convert the input to a normal spreadsheet like this:

1. Click on the "A" column marker to highlight the first column.
2. Choose Data -> Text to Columns.
3. Choose "Delimited" and click Next.
4. Make sure "Comma" is checked and click Finish.
5. Adjust the column widths until you can see the data correctly.

How ITS Uses the Secunia CSI Agent Data

The ITS Secunia administrators use the data returned from the CSI Agents to prepare third-party application installers. These installers are placed on the ISU WSUS server, sus.iastate.edu, and made available to machines in the client-side targeting groups SCPlusSecunia, DriversPlusSecunia and AllPlusSecunia. We do not choose which patches to include, but attempt to provide all those indicated by Secunia with the following exceptions:

1. **Known incompatibities with ISU services.** For example, the version of Filezilla used at ISU is listed by Secunia as end-of-life with a level 4 ("Highly critical") criticality level. However, the

current version is incompatible with Kerberos and will not work with the ISU Kerberized ftp servers. For that reason, we do not provide the current Filezilla package through WSUS.

2. **Cases where a single download package cannot be created automatically.** As an example, in the case of PHP, Secunia simply directs you to the download page for PHP. To install, you must choose between 32 and 64-bit versions, thread-safe vs. non-thread-safe version, etc. In this case we are unable to create a single installer package that can work with all machines. This is required for use with the SUS server, and so we cannot create an update package.

We currently exclude the following applications from patching:

Package	Reason for exclusion
Filezilla	New version is incompatible with ISU services.
PHP	Cannot create single installer
RealPlayer	Cannot create single installer
VMWare Server	Cannot create single installer
WireShark	Cannot create single installer

In some cases we provide multiple versions of the same package. This occurs when the package manufacturer provides multiple "current" versions of the same program. For example, Adobe continues to provide security updates for Adobe Reader versions 8, 9 and X. We have seen incompatibilities between later versions of Reader and some applications. Because of that, as long as Adobe provides security updates for earlier versions, we will provide update packages for those versions. However, when an older version reaches end-of-life and is no longer supported by the manufacturer, we will provide an upgrade package to upgrade the older version to a later version.

Acknowledgment

Thanks to Steven Spencer from LAS, who figured out that simply running the CSI Agent software did not put the necessary information into the Registry to allow the agent to make the connection to the Secunia server and determined a proper manual installation procedure.

Appendix A

Manual Configuration for Use of Secunia Updates

If for some reason you want to use the Secunia updates through the WSUS server but don't want to use Group Policy or the ITS installation package, or if you just want to know what they do, here are instructions to configure a machine for Secunia manually. You will need to download the SecuniaWSUSCertificate.cer from \\software.iastate.edu\ccsg\Secunia\SecuniaWSUSCertificate.cer to your machine.

1. Choose Start -> Run.
2. Enter
   ```
   mmc{Enter}
   ```
3. Choose File -> Add/Remove Snap-in…
4. Click Add.
5. Highlight "Certificates" and click Add.
6. Highlight "Computer account" and click Next.
7. Click Finish.
8. You'll be returned to the Add Standalone Snap-in dialog. Highlight "Group Policy Object Editor" and click Add.
9. Click Finish, then Close.
10. You'll be returned to the Add/Remove Snap-in dialog. Click OK.
11. Under "Console Root" you'll see two folders: "Certificates (Local Computer)" and "Local Computer Policy". Open "Certificates (Local Computer)".
12. Right-click on "Trusted Root Certification Authorities" and choose All Tasks -> Import.
13. Click Next, then click Browse and navigate to the certificate file you downloaded.
14. Click Next, click Next again, then click Finish.
15. Right-click on "Trusted Publishers" and choose All Tasks -> Import.
16. Click Next, then click Browse and navigate to the certificate file you downloaded.
17. Click Next, click Next again, then click Finish.
18. In the left pane under Console Root, open "Local Computer Policy".
19. Open "Computer Configuration".
20. Open "Administrative Templates".
21. Open "Windows Components".
22. Highlight "Windows Update".
23. In the right pane, open "Specify intranet Microsoft update service location".
24. In the dialog that opens, click "Enabled" and fill in the following information:
    Set the intranet update service for detecting updates: http://sus.iastate.edu
    Set the intranet statistics server: http://sus.iastate.edu
25. Click OK.
26. Open "Enable client-side targeting".
27. Click "Enabled", and under "Target group name for this computer" enter the name of the client-side target group you've chosen for this machine (usually "SCPlusSecunia").

28. Click OK.
29. Open “Allow signed content from intranet Microsoft update service location”.
30. Click “Enabled”, then click OK.
31. Close the MMC window; it is not necessary to save the changes.
32. Restart your machine to put the changes you’ve made into effect.

The Secunia CSI Agent will be installed as a service on the machine at the next Windows Update. Like the automated installs, this process does not configure Automatic Updates. You must do that by another process.

Appendix B

CSIA Command-line Options

When run from the command line, the CSI Agent (csia.exe) can accept a number of options. You can read them with the command `csia –h`. They are reproduced below.

--- Program Options: ---	
-i/--install [interval]	Install as a service checking in with the Secunia Customer Area at the specified time interval. This setting is in the format INTEGER followed by M/H/D representing minutes, hours, or days. E.g. 10M for a 10 minute interval, or 2H for a two hour interval.
-r/--remove	Remove service
-c/--cli	Run software inspection from the command line using, server-supplied settings, command-line settings, registry settings
-cc/--cli-cli	Run software inspection from the command line, using only command-line settings. Ignores registry and server-supplied settings.
--dry-run	Run the program until the point of inspection, and exit. Useful with -c -v to see configuration
-R/--runas <user[:pass]>	Specify the user the service should run as; for a domain user type "user@domain"
-L/--localservice	Run the service as the LocalService user
-N/--no-registry-write	With -i, does not write any settings to registry. With -r, does not delete settings from registry
-A/--network-appliance	Run in Network Appliance mode.
-S/--only-save-settings	Only save settings from command-line to registry, as the current user. Does not scan, install or remove
-Z/--only-delete-settings	Only delete settings from registry, as the current user. Does not scan, install or remove
-V/--version	Display program version information and exit
-h/--help	Display this message and exit
-d/--debug <file>	Write diagnostic information to the specified file.
-v/--verbose	Display additional diagnostic information
-ox/--output-xml <file>	Output inspection results to XML file
-oc/--output-csv <file>	Output inspection results to CSV file
-p/--copy <dest>	Before installing, copy executable file to <dest> and install the service to run from <dest>.
--- Scan Options: ---	
-w/--no-win-update	Do not connect to Windows Update
-t/--type <type>	Software Inspection Type: 1 (Default), 2, or 3 1: Inspect applications in default locations only 2: Inspect applications in non-default locations 3: Inspect all .dll, .exe., and .ocx files

--- Customer Area Options: ---	
-g/--group <group>	Create device as a member of <group> in your Secunia Customer Area Account (defaults to domain or langroup if unspecified)
--- Security Options: ---	
--ignore-cn	Ignore Invalid SSL Certificate Common Name (CN)
--ignore-ca	Ignore Unknown SSL Certificate Authority (CA)
--ignore-crl	Ignore SSL Certificate Revocation Check
--- Connectivity Options: ---	
-rt/-requesttimeout <minutes>	Sets a timeout on network connections 0 means no timeout, or 1-10 minutes
-x/--proxy <host[:port]>	Use HTTP proxy on given port
-U/--proxy-user <user[:pass]>	Specify Proxy authentication
-D/--direct-connection	Force direct connection, overriding default internet proxy settings