Windows Administrators Meeting
September 9, 2011
Notes (taken by Jeff Balvanz [ITSYS] and Steve Kunz [ITSYS])

Meeting Started (9:00)

Announcements

- **Account suspensions:** Steve Kunz [ITSYS] announced that account suspensions will take place October 11. Email notifications will be sent to the account holders September 13. Make sure you renew any accounts you sponsor prior to October 11.

Secunia CSI [Jeff Balvanz - ITSYS]

Jeff Balvanz [ITSYS] talked about using Secunia CSI at ISU. Secunia offers two versions of their software – Secunia PSI (Personal Software Inspector) and Secunia CSI (Corporate Software Inspector). ITS has licensed the corporate product. [The following section of notes is basically Jeff's PowerPoint text from the meeting – SLK]

Overview

- What can Secunia do for me?
- How does it work?
- How do I use it?

What can Secunia do for me?

- Provide vulnerability information about third-party software installed on your Windows computers;
- Use WSUS to provide third-party software updates via Windows Update. You do not need to know how to use Group Policy, and your machines do not have to be on the IASTATE domain. (You do have to use the central WSUS server.)

How does it work?

- Agent software on your machine inventories your installed applications;
- ITS admins use the aggregated inventory with vulnerability information from Secunia to create patch packages;
- The patch packages are put on the WSUS server;
- Machines install the patches as part of Windows Update.

Agent software

- 688K package
- Install as a service via Group Policy – apply GPOs to your OU
- Install as a service via ITS deployment package – machines don't have to use Group Policy or be on the IASTATE domain
- Install as a service manually – if you just want reporting
- Run as a scheduled task – if you don't want to waste the RAM

ITS creates patches

- Agent reports to Secunia
- Secunia CSI console collects information about insecure software and creating patches
- ITS Secunia admins assemble patches and post them to the WSUS server
- The ITS Secunia admins will not assemble patches for products that cannot be delivered as a "one package does all" installer (i.e. when you need to make a 32/64bit decision when selecting the installer). The current list of products for which ITS will not assemble patches is WireShark, RealPlayer, PHP, VMware server, Shockwave, and Google Chrome.
- ITS is aware of at least one update (FileZilla) that should NOT be distributed at ISU since the later versions break functionality.

Machines install patches as part of Windows Update

- Machines receive Microsoft updates from the local WSUS server (sus.iastate.edu)
- Machines using Secunia belong to client-side targeting groups
  –SCPlusSecunia
  –NoDriversPlusSecunia
  –AllPlusSecunia
- In those groups, Secunia patches are installed along with Windows updates according to your Automatic Update settings.

Getting Started

- Get the Secunia for ISU IT Staff document
- Install Secunia CSI on your machines using either
  –Group Policy
  –Manual installation
- Notify secunia-admins which machines you want reports on

If you use Group Policy

- Apply the appropriate GPOs to your OU (or create your own)
- Send secunia-admins@iastate.edu the name of your OU (or OUs)
- Secunia updates will be applied as part of Windows Updates
- You'll receive regular reports on your machines

If you don't use Group Policy or are on another domain:

- Run the Secunia Deployment package (or create your own)
- Send secunia-admins@iastate.edu a list of the NetBIOS names of the machines you manage
- Secunia updates will be applied as part of Windows Updates
- You'll receive regular reports on your machines

Secunia CSI is currently being used on about 750 ITS desktop systems (plus a couple other departments experimenting with it).

Secunia CSI reports all findings at a repository in Demark (you probably don't want to use this if that bothers you).

Secunia CSI is only licensed for use on systems owned by Iowa State University.

For more information (the TechNote contains the most valuable info):

- ITS TechNote: "Secunia for ISU IT Staff: Secunia CSI Reporting and Updating at Iowa State University" http://tech.its.iastate.edu/windows/admin/SecuniaGuide.pdf
- Secunia corporate web site: http://secunia.com
- Email: ITS Secunia Admin: secunia-admins@iastate.edu

Open Discussion

No time was available for open discussion.

Meeting Adjourned (10:00)

Next meeting is scheduled for October 14 (provided a sufficient agenda exists).