Security Issue: Patching pcAnywhere’s vulnerabilities with Software Management in Symantec Management Platform

# Introduction

Recent news revealed source code theft from Symantec back in 2006. At the time this article was published, only one product still contained code that the source code revealed vulnerabilities: pcAnywhere. The current version of pcAnywhere is safe from these vulnerabilities as long as the correct patches are applied. This document details how to patch the pcAnywhere agents to resolve these vulnerabilities and properly secure the software, using Symantec’s Software Management Solution, part of the Symantec Management Platform with a qualifying suite.

The purpose of this article is to make the patching as seamless and painless as possible. This process will let Software Management’s intelligent software worry about what systems have pcAnywhere installed, which have the correct version for the patches, and whether or not those patches are applied. If they are not applied, they will automatically apply them.

*Note: This document was created to patch versions 12.5 and 12.6, however by tweaking the Applicability Rule to include any other versions, you can also patch non Solution installs.*

# Prerequisites

To use the process outlined in this document, there are a few fundamental requirements. If you have a working Symantec Management Platform environment with installed agents and plug-ins, and you are currently using Software Management, there are no additional requirements.

* The Symantec Management Platform must be installed and configured in the environment. If you do not have this installed you should contact your Symantec Sales Representative to discuss if you own and/or could use this in your environment.  
  *Note: installing and using this software brings a very wide variety of management options, but requires an investment to setup and rollout.*
* The Symantec Management Agent must be installed on all systems you wish to Patch using this method.
* Within the Symantec Management Agent, the Software Management Solution agent must be installed in order to utilize the Managed Delivery Policy used in this process.

# Creating Software Resource/Package

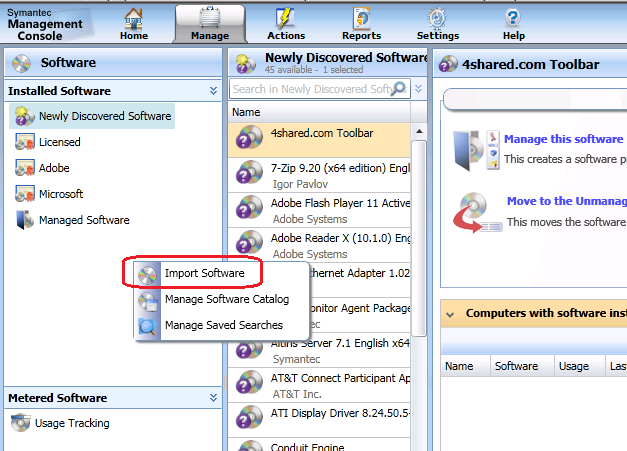
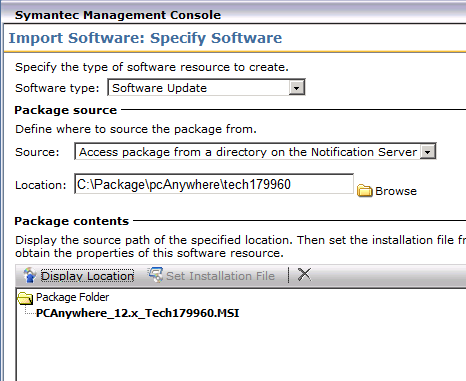
Software Resources are defined as a software component. These can be full installs, updates, or service packs. As there is a cumulative update to apply, we will create one Software Resource of the Updates type.

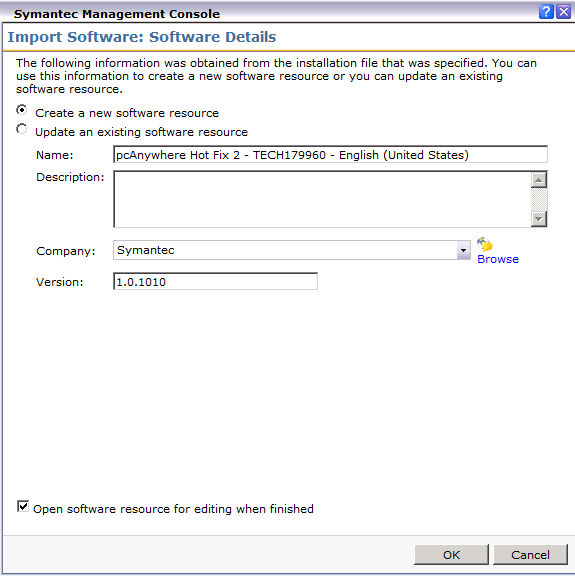
First, it is necessary to obtain the required files for the patching. Download the necessary MSI from its location within the SymWise Symantec Knowledgebase:

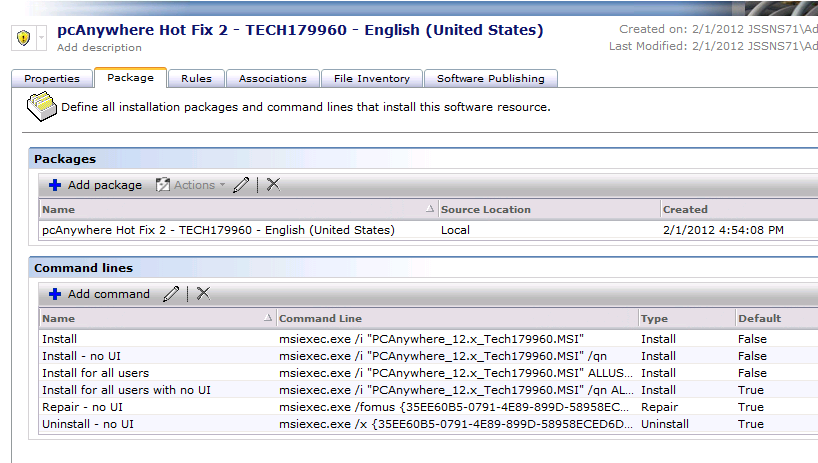
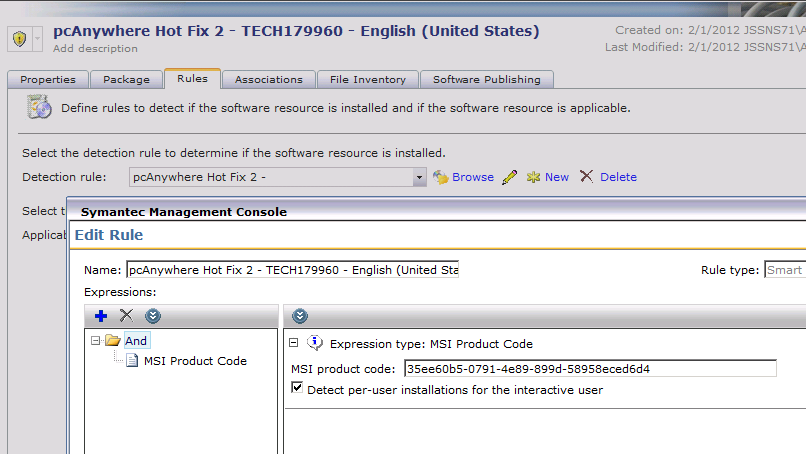
* 1. <http://www.symantec.com/docs/TECH179960>

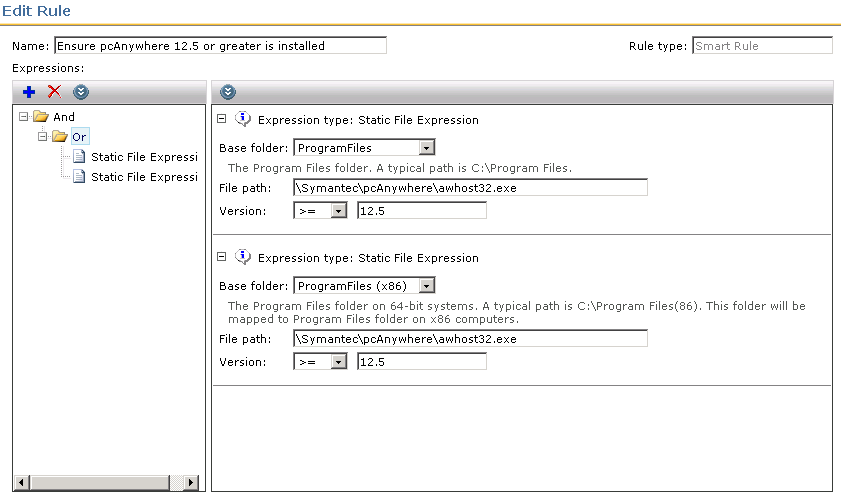
Create a folder where you typically keep your packages. If you are unsure, create it on the Notification Server directly. Place the MSI in the folder. For this example I will use: C:\Package\pcAnywhere\tech179960.

The patch is found in KB TECH179960. The following steps walk through the recommended way to create this resource, using the intelligent “Import” function.

1. In the Symantec Management Console, browse under Manage > Software > and in the upper right pane right-click in the white space and choose Import Software:  
     
   Or, if you are running version 7.0, browse to Software  >  Software Catalog  > Deliverable Software  > Updates and Service Packs then click Import.
2. In the next screen, change the Software type to: Software Update.
3. (Disregard this step if you are using your own Package settings) Change the Package Source to “Access package from a directory on the Notification Server”.
4. Browse to the location you placed the patch MSI.
5. Click Display Location to ensure the Package is properly defined, as shown:  
   
6. Click Next.
7. The following screen should be pre-populated with the following settings:
   1. Create a new software resource (radial selected)
   2. Name: pcAnywhere Hot Fix 2 – TECH179960 – English (United States)
   3. Company: Symantec
   4. Version: 1.0.1010
   5. Check box selected: Open software resource for editing when finished.



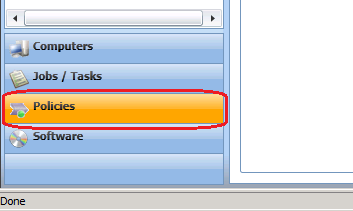
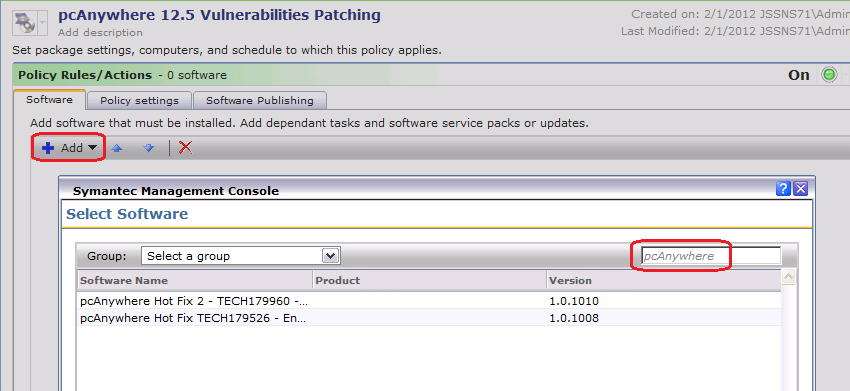
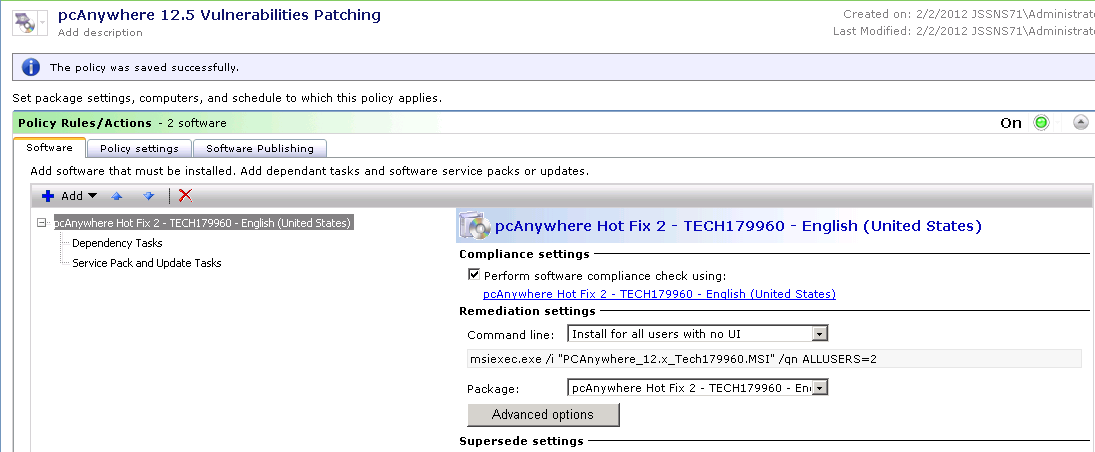
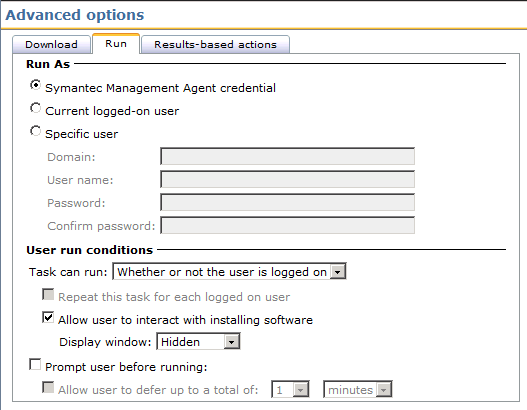
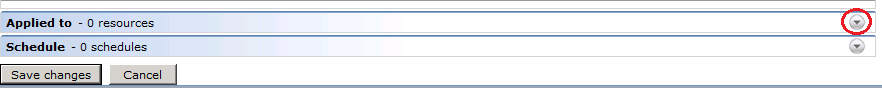
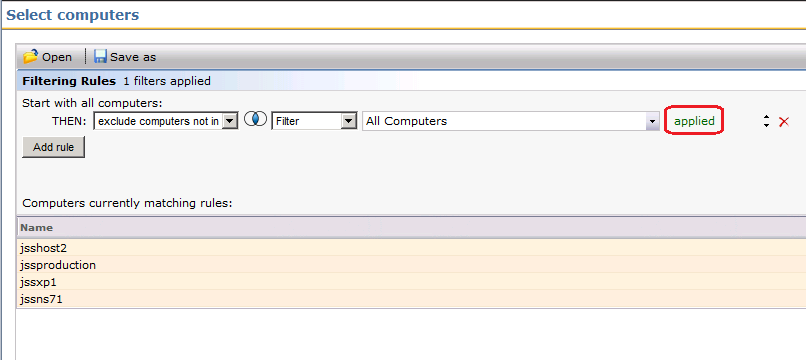
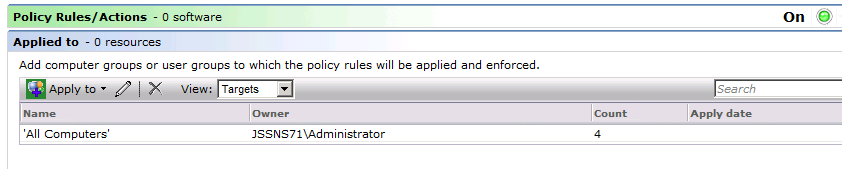
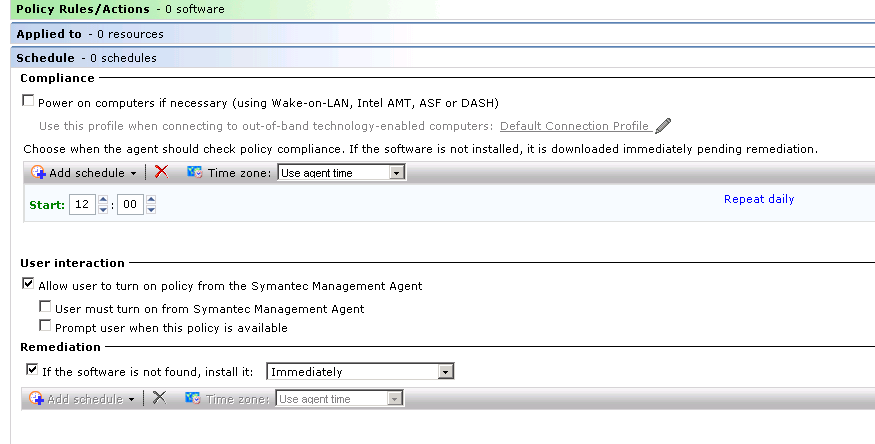
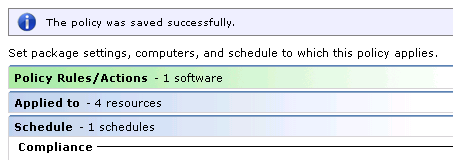
1. Click OK.
2. In the resulting window, click on the Package tab.
3. Within the Package tab all standard command-lines will have been auto-generated by the import. Typically you’ll want to use the “Install for all users with no UI” to ensure the update does not interrupt end-users.  
   
4. Click on the Rules tab.
5. The default Detection Rule is the MSI Product code of the installer and should be very specific for this Patch. If you click on the Edit icon you’ll see the below details:  
   
6. Back at the Rules tab click the New icon next to Applicability Rule.
7. Provide a name, such as “Ensure pcAnywhere 12.5 or Greater is installed”.
8. Click the blue + icon (add Rule) and choose Operator > Or.
9. Right-click on the added Or operator and choose Add > Smart Rule: Static File Expression.
10. Provide the following details:
    1. Base folder: ProgramFiles
    2. File path: Symantec\pcAnywhere\awhost32.exe
    3. Version: >= 12.5
11. Click OK to add the rule.
12. Right-click on the added Or operator and choose Add > Smart Rule: Static File Expression.
13. Provide the following details:
    1. Base folder: ProgramFiles (x86)
    2. File path: Symantec\pcAnywhere\awhost32.exe
    3. Version: >= 12.5
14. Click OK to add the rule, as shown:



1. Click OK to apply the Rule to the Resource.
2. Click Ok on the main Resource page to apply the changes.

Done! Now the Resource is created and configured to deliver the patch to all target systems. Next I will cover how to create the configure the policy that will be used to roll this out.

# Creating the Managed Policy

1. Back at the main Symantec Management Console, click the Policies link in the lower left, as shown:  
     
   Or , if you are using version 7.0, go to Manage > Policies.
2. Use the tree in the upper left to browse under Software > Managed Software Delivery.
3. Right-click on Managed Software Delivery and choose New > Managed Software Delivery.
4. At the top of the policy, click on the name shown in bold dark blue and provide a proper name, such as: pcAnywhere 12 Vulnerabilities Patching.
5. Though these subsequent steps may seem backwards, it follows the user-interface flow as we move down the policy configuration pages.
6. On the bar labeled Policy Rules / Actions to the right click the dropdown for Off and switch it to On.
7. Under the section Policy Rules / Actions click Add > Software Resource.
8. In the search field, find the first Software Resource by typing pcAnywhere, as shown:  
   
9. Select the resource named pcAnywhere Hot Fix 2 – TECH179960 – English (United States).
10. Click OK to add this resource to the Managed Delivery Policy.
11. You should now see the patch in the list, as shown in this screenshot:  
    
12. Select the update in the list and click the Advanced options button.
13. Click on the Run tab.
14. It is recommended to use the following settings:
    1. Run as > Symantec Management Agent credential
    2. Task can run: Whether or not the user is logged on
    3. Allow user to interact with installing software (checked)
    4. Display Window: Hidden.  
       
15. All other settings in these tabs can be left at the default.
16. Click OK to apply any changes.
17. Down below the Policy Rules / Actions section, expand the Applied to section by clicking on the down arrow at the far right of the section bar, as shown:  
    
18. Click the Apply to button and select Computers.
19. Click the Add rule button.
20. Change the THEN: dropdown to “exclude computers not in”.  
    *Note: The label above this section: Start with all computers:… necessitates the use of the double-negative. It makes logical sense, although it is not intuitive.*
21. Leave the middle qualifier as “Filter” and use the search dropdown to find “All Computers”.
22. Click the Update results button to ensure the filter was properly applied, as shown:  
    
23. Click OK to apply the new filter of computers.
24. Back on the main policy page it will show a row, including a Count. This count should be equal to the number of Windows systems managed by the Symantec Management Platform:  
    
25. NOTE! There are other filters that can be used, based on your environment. For example you may already have a filter that contains all systems that have the pcAnywhere agent installed, so that filter can be used in the same manner as All Computers. The reason I am not particular about who is targeted is the Applicability and Detection Rules we added to the resources. If a system does not have the pcAnywhere agent, the applicability rule will stop the remediation action from firing.
26. Next, click the dropdown arrow next to the Schedule section.
27. The first schedule is for the detection check and download (if the detection check determines that the patches are required). As this is a Managed Delivery Policy, you can set the compliance check to a repeating schedule to ensure your systems stay in compliance with the patches.
28. Click Add Schedule under the Compliance section, and choose Scheduled Time.
29. Set the time for a reasonable time where the systems can be patched. Since we will be using the silent switch, I’m setting this example at Noon (12:00). Note that the time is in military time, so schedule accordingly.
30. Click on the link labeled “no repeat” and choose Day from the resulting list. Note again that this will only run the detection check repeatedly, and after the first time it will be found in compliance, unless the system has had the patch removed wherein it will run all checks and install accordingly.
31. Keep the option checked “Allow user to turn on policy from the Symantec Management Agent”. It useful to have this policy in the UI.
32. For this example I’m leaving the remediation where the patches are applied to “immediately”. A secondary scheduled time can be added if you wish the detection check and download to occur at a different time than the patch executions.  
    
33. At the bottom of the Policy screen click “Save changes”. The Policy is now available!
34. Note that the numbers in the section bars will not show correctly until after the policy is saved, as shown in this screenshot:  
    

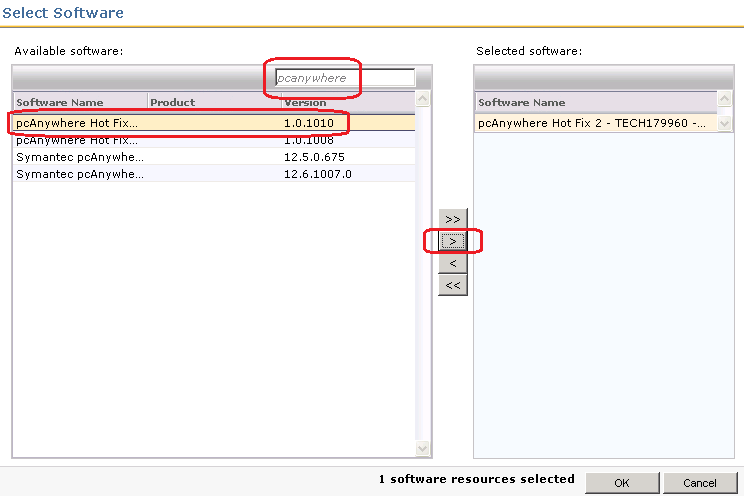
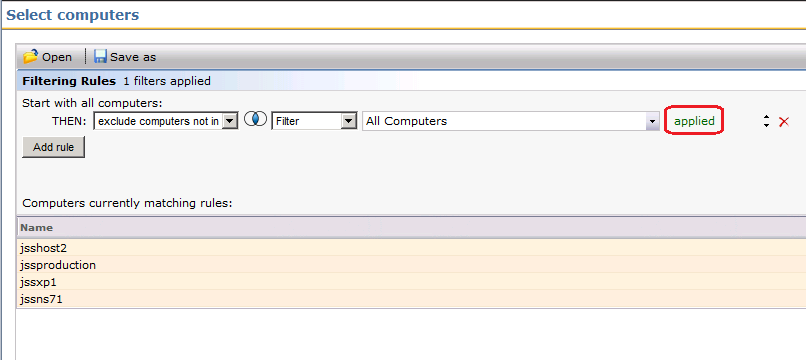
The targeted systems will get the policy when they next check for a configuration from the Symantec Management server.

# Reporting

There are two ways to report on the application of the patch. The first is a Compliance report that will give the results of the Policy execution on targeted systems. The first is to use the Installed Software report. The second adds the results of the Installed Software report with a specific Targeted Inventory Policy. Both these methods require a policy or policies to be run after the patches are applied.

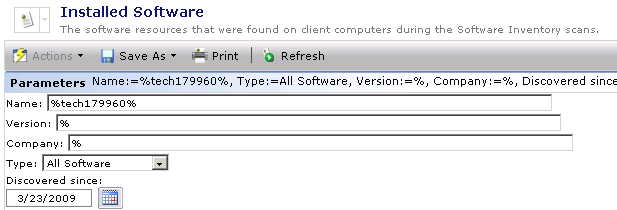
## Targeted Inventory Policy

This will employ the same Detection Rule we setup during the creation of the pcAnywhere Patch Software Resource. This Policy is part of Inventory Solution. To create the policy, follow these steps:

1. In the Symantec Management Console, browse under Manage > Policies.
2. In the left-hand tree, browse under Discovery and Inventory > Targeted Software Inventory.
3. Right-click on the Targeted Software Inventory folder and choose New > Targeted Software Inventory.
4. Provide a Name, such as: Inventory for the pcAnywhere patches TECH179960.
5. On the Software to Inventory bar change the status from Off to On.
6. In the section below, click on Select Software.
7. Use the search field to find the Software Resource we created and add it as shown:  
   
8. Click OK to save the selection.
9. Below the Software to inventory section, expand the Applied to section by clicking on the down arrow at the far right of the section bar.
10. The default filter used for these policies is all systems that have the Inventory Plug-in Installed. This usually suffices, but if you want to add your own filter, see this example:
11. Click the Apply to button and select Computers.
12. Click the Add rule button.
13. Change the THEN: dropdown to “exclude computers not in”.  
    Leave the middle qualifier as “Filter” and use the search dropdown to find “All Computers”.
14. Click the Update results button to ensure the filter was properly applied, as shown:  
    
15. Click OK to apply the new filter of computers.
16. As previously mentioned there are other filters that can be used, based on your environment.
17. Next, click the dropdown arrow next to the Schedule section.
18. Click Add Schedule and choose Scheduled Time.
19. Set the time for a reasonable time where the systems can be inventoried. Since this is a very non-intrusive inventory (scans the one detection rule) I’m setting this example at Noon (12:00). Note that the time is in military time, so schedule accordingly.
20. Click on the link labeled “no repeat” and choose Daily from the resulting list. This will give you frequent data so you can be up to date on what systems have or do not have this patch applied.
21. The Policy should now be complete, as shown:  
    
22. Now targeted systems will run this inventory once daily to check and see if the fixes are applied.

## Installed Software

This report works best if you are using 7.1 SP2. He following steps walk through how to find, configure, and run this report:

1. In the Symantec Management Console browse under Reports > All Reports > Discovery and Inventory > Inventory > Cross-platform > Software\Applications > Software > and select Installed Software.
2. In the parameters section, use the following:
   1. Name: %tech179960%
   2. Version: %
   3. Company: %
   4. Type: All Software
   5. Discovered Since: wind this back several years to ensure the report provides all data.  
      
3. Click the Refresh button to run the report.
4. The row that returns can be double-clicked on (or right-click option) to drill down and show all systems that now have this patch applied.

# Conclusion

This should give you the tools needed to effectively patch your pcAnywhere agents/plug-ins to ensure you are protected from any security vulnerabilities. The steps and settings proposed here are not the only way to accomplish this, but provide a solid example of how Software Management can accomplish the needed task.