

[NT] pcAnywhere Allows Local Users to Become SYSTEM

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0067.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/17/03

To: list@securiteam.com

Date: 17 Nov 2003 11:49:54 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

pcAnywhere Allows Local Users to Become SYSTEM

SUMMARY

<<http://www.symantec.com/pcanywhere/>> pcAnywhere is an industry-leading remote control software that features remote management paired with file transfer capabilities. pcAnywhere has the ability to help quickly resolve helpdesk and server support issues.

DETAILS

Vulnerable systems:

* Symantec pcAnywhere version 10.x and 11.x

When pcAnywhere is started as a service or set to launch with windows an attacker may be able to take SYSTEM rights via the help interface. AWHOST32.exe runs as the user SYSTEM while interacting with the local desktop on the machine that pcAnywhere is listening. Users have the ability to control AWHOST32 via an icon in the Windows systray.

Brett Moore of security-assessment.com pointed out a flaw in the Win32 help API which can be found at

<<http://www.securiteam.com/windowsntfocus/6W00P1P8KC.html>> HTML Help API –

Securiteam: [NT] pcAnywhere Allows Local Users to Become SYSTEM

Privilege Escalation. A variation of this attack is present in both pcAnywhere 10 and 11. It is unknown how this issue affects older versions of pcAnywhere since they are no longer supported products.

In order to exploit this issue you must open pcAnywhere and configure it accordingly. Right click on your "Host" icon and choose properties. Click the settings tab at the top and then check either "Run as a service" or "Launch with Windows". Apply all settings and reboot your machine. After the machine is back up you should login as a user with minimal rights to the local machine.

Opening the Windows Task Manager would reveal the AWHOST32 process running as SYSTEM. At this point you should also see the pcAnywhere icon in the task bar that indicates a "Host" is listening. If you right click on the "Host" icon you have the option to choose "help". Once you open the pcAnywhere help you should note that in the process list winhlp32 is running as SYSTEM.

From this point you have a few options for local exploitation. If you click "File" followed by "open" winhlp32 will prompt you to browse for a hlp file. Rather than looking for a help file we can replace the "*.hlp" in the filename box with "*". You should now be able to see all files on the system that are available to the user SYSTEM. One technique would be to browse to the local SAM file and simply right click on it and change the NTFS permissions. Another technique would be to browse to c:\windows\system32 and right click on cmd.exe and choose "open". This will drop you to a command prompt running as SYSTEM.

For version 11 of pcAnywhere hh.exe is used in place of winhlp32.exe. This opens up the exploitation path pointed out by Brett Moore as well as one that KF discovered. If you right click on the pcAnywhere icon and choose help, rather than choosing "file" then "open" you should right click on the help topic that is currently being displayed. You should be given the option to "view source". Upon clicking "view source" you will be presented with a windows notepad session. At this point in time notepad.exe is running as SYSTEM... exploitation from here is similar to the notes mentioned above.

This issue poses a risk for machines that run pcAnywhere because other local users can interact with the systray icon. It also poses a risk for machines that allow remote access via pcAnywhere, once logged in regardless of the user's rights they should be able to interact with the systray icon and potentially take SYSTEM rights.

Vendor Status:

Symantec verified this vulnerability does exist in the service-mode configuration of currently supported releases of Symantec pcAnywhere. This issue has been rectified and fixes are available via LiveUpdate to Symantec pcAnywhere.

Securiteam: [NT] pcAnywhere Allows Local Users to Become SYSTEM

Mitigating Circumstances:

While this potentially is a high-risk vulnerability, there are various mitigating circumstances that greatly reduce the risk of intentional or inadvertent exploitation of this weakness in Symantec pcAnywhere.

- * Symantec pcAnywhere must first be configured as a service by an admin-level user, launched and running on the machine BEFORE a non-privileged user could exploit this vulnerability

- o If the host service is not running when the non-privileged user logs on the machine in question, they have NO ABILITY to configure and launch Symantec pcAnywhere in a manner where this exploit will be present

- o Setting up the Symantec pcAnywhere Host service (and launching it) requires administrative privileges

- * The user must have a user-account on the host system and be logged on interactively to exploit this issue

- * This issue cannot be exploited remotely

- * System privileges can be gained only on the local system, which normally limits the impact to the user system

- * Although Symantec pcAnywhere allows remote control and management of other systems, additional identification and authentication is required by default to gain access to any remotely managed systems

- o Just gaining SYSTEM-level access on the local host does not provide additional access to any remote system(s) through Symantec pcAnywhere

- * Access to remote administration capability should normally be restricted to trusted Administrators only with additional restricted access to the physical host system(s)

Symantec strongly recommends all users of supported versions of Symantec pcAnywhere update to the latest LiveUpdate packages to prevent potential misuse of this local access weakness.

ADDITIONAL INFORMATION

The original advisory is available from:

<<http://www.secnetops.com/research/advisories/SRT2003-11-13-0218.txt>>
<http://www.secnetops.com/research/advisories/SRT2003-11-13-0218.txt>.

The information has been provided by <mailto:dotslash@snoft.com> KF.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[NT] pcAnywhere Allows Local Users to Become SYSTEM

Securiteam: [NT] pcAnywhere Allows Local Users to Become SYSTEM

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.