



SA#: 01-26-12

Security Alert! Symantec - pcAnywhere

This week, Symantec took the highly unusual step of telling users of its pcAnywhere remote access software to either disable or uninstall the software while it fixes a number of security vulnerabilities.

Symantec's recommendation was blunt.

"At this time, Symantec recommends disabling the product until we release a final set of software updates that resolve currently known vulnerability risks," the company stated Wednesday 1-25-12..

The advice to yank pcAnywhere from service was prompted by a 2006 leak of its source code and the recent involvement of "Anonymous", the loosely-organized group of hackers whose latest exploit was to cripple several government websites after U.S. authorities accused executives of the Megaupload file-sharing service with widespread copyright infringement.

Last week, Symantec admitted its own network had been breached in 2006. Tuesday, 1-24-12, it again said source code for several of its products, including pcAnywhere, had been stolen at that time.

Anonymous claims to have reverse engineered the pcAnywhere client to bypass authentication and are taking over corporate pcAnywhere servers.

MICROS Systems, Inc. (MICROS) strongly recommends that any of its customers using the Symantec pcAnywhere software immediately disable or uninstall the software until such time as Symantec has released fixes for its security vulnerabilities. The MICROS Remote Support Policy is posted on our public Information Security web site at the link below:

http://www.micros.com/NR/rdonlyres/35B1DED6-6D56-48E6-98A2-D0C58C34AD2E/0/REMOTE_SUPPORT_POLICY_060910.pdf

This policy has, for many years, instructed MICROS customers to disable their remote access applications/tools, such as pcAnywhere, except when temporarily needed for a specific purpose.

MICROS has also published a November 2005 advisory on its Information Security web site instructing pcAnywhere users how to disable/enable the pcAnywhere application and to change user accounts and passwords. The link to this advisory is below:

<http://www.micros.com/NR/rdonlyres/E32ADCBE-5204-4CF2-9D4C-DC031C6C0FDB/0/CreditCardNotice1105A.pdf>

Please contact your MICROS representative if you have any questions.

MICROS Systems, Inc. Information Security Department