



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

January 27, 2012

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2012-004

DATE(S) ISSUED:
01/26/2012
01/27/2012 - Updated

SUBJECT:
Vulnerability in Symantec pcAnywhere Could Allow Remote Code Execution

ORIGINAL OVERVIEW:
A vulnerability has been discovered in Symantec pcAnywhere which could allow remote code execution. pcAnywhere is a remote access software solution. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Symantec has released a statement indicating that users should not use pcAnywhere or at minimum block the ports used by pcAnywhere at the perimeter. This is due to a breach in which the source code for various products was stolen. Symantec indicated that pcAnywhere is the only product that has not been fixed since the breach. There is a potential for additional vulnerabilities to be exploited due to this breach.

January 27 UPDATED OVERVIEW:
Symantec has released an update which that addresses this vulnerability in versions 12.0 and 12.1 of the pcAnywhere software.

SYSTEMS AFFECTED:

- pcAnywhere 12.5.3
- pcAnywhere 12.5 SP1
- pcAnywhere 12.5
- pcAnywhere 12.1
- pcAnywhere 12.0

RISK:**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Medium**ORIGINAL DESCRIPTION:**

Symantec pcAnywhere is prone to a remote code-execution vulnerability because it fails to properly validate and filter input during the login and authentication process. To remotely exploit this vulnerability, an attacker would have to send a specially crafted request to a vulnerable system running the software over port 5631/TCP. When the application processes the request, the exploit is triggered.

Successful exploitation may result in an attacker gaining the same privileges assigned to the application, which is System under most installations. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Symantec has released a Hot Fix that mitigates the issue in version 12.5 of the software. If the application is configured to receive updates via LiveUpdate, this update will be automatically applied to each vulnerable system when LiveUpdate is run. Information regarding this hot fix can be obtained from the following

site: <http://www.symantec.com/business/support/index?page=content&id=TECH179526>

~~Symantec also plans on releasing fixes that will mitigate the issue in versions 12.1 and 12.0 as well. However, no fixes are available for these versions at this time.~~

Symantec has released a statement indicating that users should not use pcAnywhere or at minimum block the ports used by pcAnywhere at the perimeter. This is due to a breach in which the source code for various products was stolen. Symantec indicated that pcAnywhere is the only product that has not been fixed since the breach. There is a potential for additional vulnerabilities to be exploited due to this breach.

January 27 UPDATED DESCRIPTION:

Symantec has released an update which that addresses this vulnerability in versions 12.0 and 12.1 of the pcAnywhere software.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Unless there is a business need, consider discontinuing use of pcAnywhere until Symantec indicates otherwise.
- Consider blocking the pcAnywhere assigned ports of 5631/TCP and 5632/UDP at the organization's perimeter unless there is a critical business need that requires they remain open.
- Apply the Hot Fix to vulnerable systems after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Symantec

http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120124_00
<http://www.symantec.com/business/support/index?page=content&id=TECH179526>
http://www.symantec.com/connect/sites/default/files/pcAnywhere%20Security%20Recommendations%20WP_01_23_Final.pdf

ComputerWorld:

[http://www.computerworld.com/s/article/9223725/Threatened by Anonymous Symantec tells users to pull pcAnywhere s plug](http://www.computerworld.com/s/article/9223725/Threatened_by_Anonymous_Symantec_tells_users_to_pull_pcAnywhere_s_plug)

CVE:

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3478>

Security Focus:

<http://www.securityfocus.com/bid/51592>