



March 15, 2007

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2007-03-15

Computer Associates BrightStor ARCserve Backup Tape Engine Multiple Vulnerabilities
CVE-2006-6076, CVE-2007-1447, CVE-2007-1448

- **Synopsis**

BrightStor ARCserve Backup provides a complete, flexible and integrated backup and recovery solution for Windows, NetWare, Linux and UNIX environments.

Three buffer overflow vulnerabilities were discovered in CA's BrightStor ARCserve TapeEngine services which could allow a remote attacker to cause arbitrary command execution or perform a Denial of Service.

- **Vulnerable System or Application**

BrightStor ARCserve Backup r11.5
BrightStor ARCserve Backup r11.1
BrightStor ARCserve Backup for Windows r11 BrightStor Enterprise Backup r10.5 BrightStor ARCserve Backup v9.01

CA Protection Suites r2
CA Server Protection Suite r2
CA Business Protection Suite r2
CA Business Protection Suite for Microsoft Small Business Server Standard Edition r2
CA Business Protection Suite for Microsoft Small Business Server Premium Edition r2

- **Vulnerability Information**

The flaws specifically exist within the Tape Engine Executable (tapeeng.exe) and are the result of incorrect handling of RPC requests on TCP port 6502. The interface is identified by 62b93df0-8b02-11ce-876c-00805f842837.

first vulnerability --- opnum 15 (CVE-2006-6076)

CA has announced that the issue CVE-2006-6076 should be fixed in QO84983, but our testing shows this vulnerability to still exist after SP2 patched QO82963&QO84983 .

A memory corruption vulnerability exists in the Tape Engine service. More specifically, the vulnerability is due to the failure of the application to check the validity of the supplied data when processing stub data of an RPC call with opnum 15. This might result in memory corruption as an attacker can provide arbitrary memory locations to be overwritten.

An unauthenticated remote attacker can exploit this vulnerability by sending a specially crafted RPC request message to the Tape Engine service. Successful exploitation may cause denial of service, or allow injection and execution of arbitrary code in the security context of the vulnerable service. The default security context of the service is normally "System".

Second vulnerability--- opnum 16 or 17 (CVE-2007-1447)

A memory corruption vulnerability exists in the Tape Engine service. More specifically, the vulnerability is due to the failure of the application to check the validity of the supplied data when processing stub data of an RPC call with opnum 16 or 17. Specifically, the vulnerable code attempts to write into the memory structure referenced by stub data without properly validating the user provided memory address. This might result in memory corruption as an attacker can provide arbitrary memory locations to be overwritten.

An unauthenticated remote attacker can exploit this vulnerability by sending a specially crafted RPC request message to the Tape Engine service. Successful exploitation may cause denial of service, or allow injection and execution of arbitrary code in the security context of the vulnerable service. The default security context of the service is normally "System".

Third vulnerability --- opnum 46 (CVE-2007-1448)

An unauthenticated remote attacker can disable the Tape Engine RPC interface by sending the Tape Engine service a specially crafted RPC request to opnum 46. Successful Denial of Service exploitation, will result in a Normal user getting the "nca_unk_if" response.

• Resolution

Please update the software
Get patches from CA website <http://supportconnectw.ca.com>

• Credits

These vulnerabilities were discovered by Wei Wang of McAfee Avert Labs.

• Legal Notice

Copyright (C) 2007 McAfee, Inc.

The information contained within this advisory is provided for the convenience of McAfee's customers, and may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in

any way. McAfee makes no representations or warranties regarding the accuracy of the information referenced in this document, or the suitability of that information for your purposes.

McAfee, Inc. and McAfee Avert Labs are registered Trademarks of McAfee, Inc. and/or its affiliated companies in the United States and/or other Countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.