LS-20060313

Computer Associates BrightStor ARCserve Backup Remote Buffer Overflow Vulnerability

Release Date:
10/05/2006

Date Reported:
04/07/2006

Severity:
Critical (Remote Code Execution)

Vendor:
Computer Associates

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

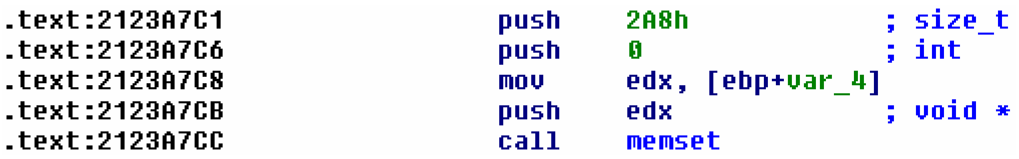
http://www3.ca.com/solutions/ProductFamily.aspx?ID=115

Systems Affected:
-BrightStor ARCserve Backup R11.5 Server
-BrightStor Enterprise Backup 10.5
-BrightStor ARCserve Backup v9.01
-CA Server Protection Suite r2
-CA Business Protection Suite r2

Overview:
LSsec has discovered a vulnerability in Computer Associates BrightStor ARCserve Backup, which could be exploited by an anonymous attacker in order to execute arbitrary code with SYSTEM privileges on an affected system. The flaw specifically exists within the Message Engine (msgeng.exe) due to incorrect handling of RPC requests on TCP port 6503. The interface is identified by dc246bf0-7a7a-11ce-9f88-00805fe43838. **Opnum 43** specifies the vulnerable operation within this interface.

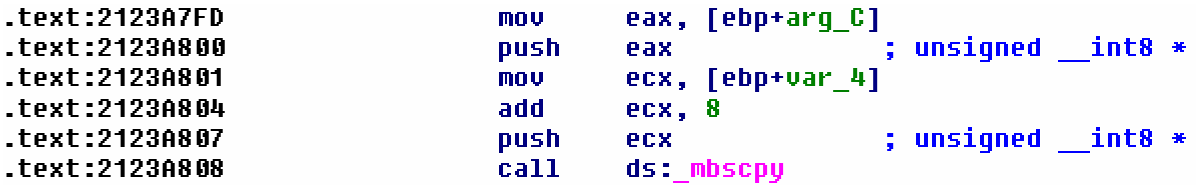
Vulnerability Details:
It is possible to trigger a heap overflow in ASCORE.dll by sending a request with 700 bytes of stub data to the vulnerable operation.

The destination is a 2A8h (680 decimal) byte heap buffer.



```
.text:2123A7C1                 push    2A8h            ; size_t
.text:2123A7C6                 push    0               ; int
.text:2123A7C8                 mov     edx, [ebp+var_4]
.text:2123A7CB                 push    edx             ; void *
.text:2123A7CC                 call    memset
```

Incongruous use of mbscpy() allows for arbitrary DWORD overwrite:



```
.text:2123A7FD                 mov     eax, [ebp+arg_C]
.text:2123A800                 push    eax             ; unsigned __int8 *
.text:2123A801                 mov     ecx, [ebp+var_4]
.text:2123A804                 add     ecx, 8
.text:2123A807                 push    ecx             ; unsigned __int8 *
.text:2123A808                 call    ds:_mbscpy
```

Execution of code can be achieved through a number of means, for instance through the UnhandledExceptionFilter or a PEB locking pointer.

Disclaimer
The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are no warranties, implied or express, with regard to this information. In no event shall the author be liable for any direct or indirect damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.