LS-20060908

Computer Associates BrightStor ARCserve Backup v11.5 Remote Buffer Overflow Vulnerability

Release Date:
12/08/2006

Date Reported:

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 < SP2

Patch:
Service Pack 2 resolves this issue

Overview:
LSsec has discovered a vulnerability in Computer **Associates BrightStor ARCserve Backup v11.5**, 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 Tape Engine (tapeeng.exe) due to incorrect handling of RPC requests on TCP port 6502. The interface is identified by **62b93df0-8b02-11ce-876c-00805f842837**. **Opnum 37** specifies the vulnerable operation within this interface.

Vulnerability Details:
TAPEENG.dll v11.5.3884.0 contains a buffer overflow vulnerability due to incongruous use of vsprintf()

```
0027C64D   LEA ECX, DWORD PTR SS:[EBP+14]          ; arglist
0027C650   PUSH ECX
0027C651   MOV EDX, DWORD PTR SS:[EBP+10]          ; fmt
0027C654   PUSH EDX
0027C655   LEA EAX, DWORD PTR SS:[EBP-1924]        ; dst
0027C65B   PUSH EAX
0027C65C   CALL DWORD PTR DS:[<&MSVCRT.vsprintf>]  ; MSVCRT.vsprintf
```

```
fmt: "RPCGetGroupStatus:: Group %s NOT available. retStatus = 0x%x, groupStatus = %u. Hence Releasing LOCK."
```

This specific flaw requires the Message Log Level to be set to either "*Detail*" or "*Detail, with Read/Writes*".

Following Log Levels are available:

0x00: None
0x01: Summary
0x02: Detail
0x03: Detail, with Read/Writes

Following Output Types are available:

0x00: Both, Screen and File
0x01: Screen Only
0x02: File Only

Each Log Level / Output Type is represented by a specific ID which is stored in the .data section of TAPEUTIL.dll and queried before data is getting logged. The Log Level ID is stored at 0x6F7410 and the Output Type at 0x6F7418.

Sending a packet with the following stub to **Opnum 43** allows us to change the Log Level remotely:

```
+00h DWORD
+04h DWORD <Log Level>
+08h DWORD <Output Type>
+0Ch DWORD
+10h DWORD
```

Copyright © 2006 LS Security
Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of LSsec. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email request@lssec.com for permission.

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.