LS-20060220

Computer Associates BrightStor ARCserve Backup Remote Buffer Overflow Vulnerability

Release Date:
10/05/2006

Date Reported:
02/20/2006

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

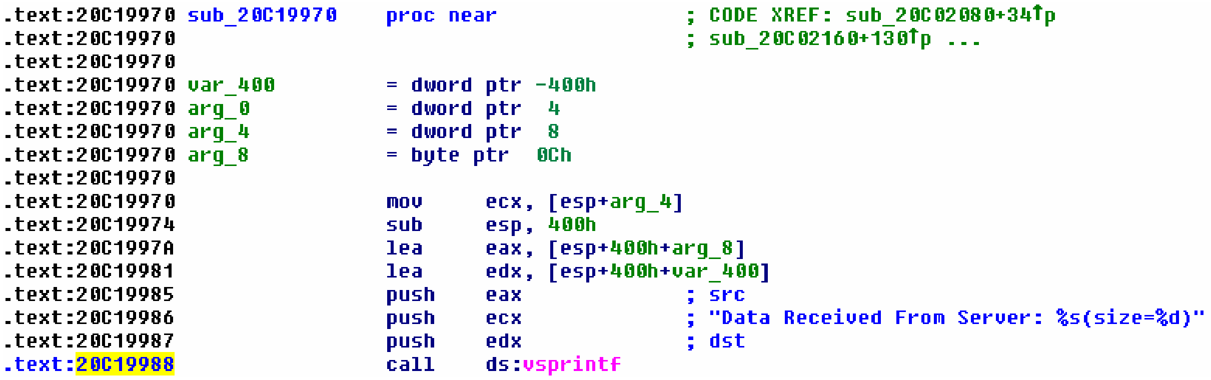
Systems Affected:
-BrightStor ARCserve Backup R11.5 Client
-BrightStor ARCserve Backup R11.5 Server
-BrightStor Enterprise Backup 10.5
-BrightStor ARCserve Backup v9.01
-CA Server Protection Suite r2
-CA Business Protection Suite r2

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 Discovery Service (casdscsvc.exe) due to incorrect handling of requests on TCP port 41523.

Vulnerability Details:
The BrightStor software will automatically detect other BrightStor (ARCserve) servers on the local network. The Discovery Service sends a packet to the broadcast address of a given subnet. Each system running the Discovery Service responds to the IP address embedded in the broadcast packet.

All systems discovered on the subnet transmit their hostnames and IP addresses and then read in the hostname of the system which initiated the broadcast.

This hostname is copied into a fixed 1024 byte stack buffer by use of an incongruous call to vsprintf() in ASBRDCST.DLL



```
.text:20C19970 sub_20C19970    proc near               ; CODE XREF: sub_20C02080+34↑p
.text:20C19970                                         ; sub_20C02160+130↑p ...
.text:20C19970
.text:20C19970 var_400         = dword ptr -400h
.text:20C19970 arg_0           = dword ptr  4
.text:20C19970 arg_4           = dword ptr  8
.text:20C19970 arg_8           = byte ptr  0Ch
.text:20C19970
.text:20C19970                 mov     ecx, [esp+arg_4]
.text:20C19974                 sub     esp, 400h
.text:20C1997A                 lea     eax, [esp+400h+arg_8]
.text:20C19981                 lea     edx, [esp+400h+var_400]
.text:20C19985                 push    eax             ; src
.text:20C19986                 push    ecx             ; "Data Received From Server: %s(size=%d)"
.text:20C19987                 push    edx             ; dst
.text:20C19988                 call    ds:vsprintf
```

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.