

LS-20061002

## Computer Associates BrightStor ARCserve Backup Remote Code Execution Vulnerability

**Release Date:**

01/11/2007

**Date Reported:**

10/04/2006

**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
- BrightStor ARCserve Backup R11.1
- BrightStor ARCserve Backup R11
- BrightStor ARCserve Backup v9.01
- BrightStor Enterprise Backup 10.5

**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 191 specifies the vulnerable operation within this interface.

**Vulnerability Details:**

This specific flaw allows for redirection of code by manipulating a variable on the stack. This variable is referenced later and can be abused in the following call:

```
00264DFE CALL DWORD PTR DS:[EAX+C] ;EAX is controllable.
```

The following code modifies the stack variable:

STACK before REP instruction

```
01C9FA2C 01C9FB84
01C9FA30 00000000 VAR
01C9FA34 02860286
01C9FA38 00000002
01C9FA3C 01C9FAD0
01C9FA40 /01C9FD48 EBP
01C9FA44 |77D96065 RETURN to RPCRT4.77D96065 from RPCRT4.77D36CB8
01C9FA48 |002A2E60 TAPEEN_1.002A2E60
```

RPCRT4

```
77D36CD9 REP MOVSD WORD PTR ES:[EDI],DWORD PTR DS:[ESI] ;Our address is stored in VAR
...
77D36CE3 MOV EAX,DWORD PTR SS:[EBP+8] ;TAPEEN_1.002A2E60
77D36CE6 CALL EAX
```

#### STACK after REP instruction

```
01C9FA2C 0014DB88
01C9FA30 00172CDC Our address
01C9FA34 02860286
01C9FA38 00000002
01C9FA3C 01C9FAD0
01C9FA40 /01C9FD48 EBP
01C9FA44 77D96065 RETURN to RPCRT4.77D96065 from RPCRT4.77D36CB8
01C9FA48 002A2E60 TAPEEN_1.002A2E60
```

#### TAPEEN\_1

```
002A2E60 MOV EAX,DWORD PTR SS:[ESP+8] ;Our address
002A2E64 PUSH EAX
002A2E65 CALL TAPEEN_1.00264DB0
```

#### STACK after CALL TAPEEN\_1.00264DB0

```
01C9FA1C /01C9FA40 EBP
01C9FA20 002A2E6A RETURN to TAPEEN_1.002A2E6A from TAPEEN_1.00264DB0
01C9FA24 00172CDC PUSHED EAX
01C9FA28 77D36CE8 RETURN to RPCRT4.77D36CE8
01C9FA2C 0014DB88
01C9FA30 00172CDC Our address
01C9FA34 02860286
01C9FA38 00000002
01C9FA3C 01C9FAD0
01C9FA40 /01C9FD48 EBP
01C9FA44 77D96065 RETURN to RPCRT4.77D96065 from RPCRT4.77D36CB8
01C9FA48 002A2E60 TAPEEN_1.002A2E60
```

#### TAPEEN\_1

```
00264DB0 PUSH EBP
00264DB1 MOV EBP,ESP
...
00264DF1 MOV ESI,DWORD PTR SS:[EBP+8] ;Our address is stored in ESI
00264DF4 MOV EAX,DWORD PTR DS:[ESI+334] ;The data referenced by ESI+334 is moved to EAX
00264DFA MOV ECX,DWORD PTR DS:[EAX+18]
00264DFD PUSH ECX
00264DFE CALL DWORD PTR DS:[EAX+C] ;The data referenced by EAX+C is called
```

### 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.