

# [NT] CA Multiple Product DBASVR RPC Server Multiple Buffer Overflow Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-10/msg00027.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 8 Oct 2006 15:55:41 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

CA Multiple Product DBASVR RPC Server Multiple Buffer Overflow Vulnerabilities

---

## SUMMARY

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Computer Associates BrightStor ARCserve Backup, Enterprise Backup, Server Protection Suite and Business Protection Suite. Authentication is not required to exploit this vulnerability and both client and servers are affected.

## DETAILS

The problem specifically exists within DBASVR.exe, the Backup Agent RPC Server. This service exposes a number of vulnerable RPC routines through a TCP endpoint with ID 88435ee0-861a-11ce-b86b-00001b27f656 on port 6071. The most trivial of the exposed vulnerabilities results in an exploitable stack overflow.

The vulnerable routines include:

```
/* opcode: 0x01, address: 0x00401A70 */
```

## [NT] CA Multiple Product DBASVR RPC Server Multiple Buffer Overflow Vulnerabilities

```
long sub_401A70 (  
[in][string] char * arg_1,  
[in][string] char * arg_2, // stack overflow  
[out][size_is(8192), length_is(*arg_4)] char * arg_3,  
[in, out] long * arg_4  
);
```

```
/* opcode: 0x02, address: 0x00401CC0*/
```

```
long sub_401CC0 (  
[in][string] char * arg_1,  
[in][string] char * arg_2, // stack overflow  
[in][string] char * arg_3,  
[out] long * arg_4  
);
```

```
/* opcode: 0x18, address: 0x004041C0*/
```

```
long sub_4041C0 (  
[in][string] char * arg_1,  
[in][string] char * arg_2, // stack overflow  
[out] long * arg_3  
);
```

The first two vulnerable subroutines are the result of inline strcpy()/memcpy()'s. The third vulnerable subroutine is due to an insecure call to lstrcat().

### Vendor Response:

Computer Associates has issued an update to correct this vulnerability.

More details can be found at:

<http://supportconnectw.ca.com/public/storage/infodocs/basbr-secnotice.asp>  
<http://supportconnectw.ca.com/public/storage/infodocs/basbr-secnotice.asp>

### CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5143>  
CVE-2006-5143

### Disclosure Timeline:

2006.03.27 – Digital Vaccine released to TippingPoint customers  
2006.03.28 – Vulnerability reported to vendor  
2006.10.05 – Coordinated public release of advisory

### ADDITIONAL INFORMATION

The information has been provided by <mailto:TSRT@xxxxxxxxx> Pedram Amini,  
TippingPoint Security Research Team.

The original article can be found at:

[NT] CA Multiple Product DBASVR RPC Server Multiple Buffer Overflow Vulnerabilities

<<http://www.tippingpoint.com/security/advisories/TSRT-06-11.html>>

<http://www.tippingpoint.com/security/advisories/TSRT-06-11.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.