

[NT] CA BrightStor ArcServe Media Server Multiple Buffer Overflow Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00031.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 25 Apr 2007 15:48:59 +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 BrightStor ArcServe Media Server Multiple Buffer Overflow Vulnerabilities

SUMMARY

A vulnerability allows attackers to execute arbitrary code on vulnerable installations of Computer Associates BrightStor ARCserve Media Server. User interaction is not required to exploit this vulnerability.

DETAILS

Vulnerable Systems:

- * BrightStor ARCserve Backup release 11.5 SP2
- * BrightStor ARCserve Backup release 11.5
- * BrightStor ARCserve Backup release 11.1
- * BrightStor ARCserve Backup release 11 for Windows
- * BrightStor Enterprise Backup release 10.5
- * BrightStor ARCserve Backup version 9.01
- * CA Server Protection Suite release 2
- * CA Business Protection Suite release 2

The specific flaw exists in the SUN RPC service which binds to a randomly chosen high TCP port. The target port can be obtained by querying the port

[NT] CA BrightStor ArcServe Media Server Multiple Buffer Overflow Vulnerabilities

mapper. Multiple stack-based buffer overflows exist during the parsing of malformed RPC strings. Exploitation of these overflows can result in arbitrary code execution.

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

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2139>
CVE-2007-2139

Disclosure Timeline:

2007.03.08 – Vulnerability reported to vendor
2007.04.19 – Digital Vaccine released to TippingPoint customers
2007.04.24 – Coordinated public release of advisory

ADDITIONAL INFORMATION

The information has been provided by <mailto:zdi-disclosures@xxxxxxxxx>
ZeroDay Initiative.

The original article can be found at:

<http://www.zerodayinitiative.com/advisories/ZDI-07-022.html>
<http://www.zerodayinitiative.com/advisories/ZDI-07-022.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.