

[NT] CA BrightStor ARCserve Backup Agent For MS SQL Server Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0026.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/07/05

To: list@securiteam.com

Date: 7 Aug 2005 18:28:22 +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 Backup Agent For MS SQL Server Buffer Overflow

SUMMARY

"BrightStor ARCserve Backup provides backup and restore protection for all classes of Windows, NetWare, Linux and UNIX servers, as well as Windows, Mac OS X, Linux, UNIX, AS/400 and VMS client environments". Remote exploitation of a buffer overflow vulnerability in Computer Associates International Inc's BrightStor ARCserve Backup UniversalAgent allow attackers to execute arbitrary code.

DETAILS

Vulnerable Systems:

* CA BrightStor ARCserve Backup Agent for Microsoft SQL Server version 11.0

When a string with a length over 3168 bytes, is sent to the listening port (6070 by default) a stack based buffer overflow occurs. Successful exploitation allows remote attackers to execute arbitrary code with SYSTEM level privileges.

Workaround:

Securiteam: [NT] CA BrightStor ARCserve Backup Agent For MS SQL Server Buffer Overflow

Restrict remote access at the network boundary, unless remote parties require service. Access to the affected host should be filtered at the network boundary if global accessibility is not required.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1272>>
CAN-2005-1272

Disclosure Timeline:

04/25/2005 – Initial vendor notification
04/25/2005 – Initial vendor response
08/02/2005 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:idlabs-advisories@idefense.com>> ideoense.

The original article can be found at:

<<http://www.ideoense.com/application/poi/display?id=287&type=vulnerabilities>>
<http://www.ideoense.com/application/poi/display?id=287&type=vulnerabilities>.

The vendor advisory can be found at:

<<http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=33239>>
<http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=33239>.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.