

[NT] Computer Associates BrightStor ARCserve/Enterprise Backup Agents Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0069.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/19/05

To: list@securiteam.com

Date: 19 Sep 2005 10:20:14 +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>

Computer Associates BrightStor ARCserve/Enterprise Backup Agents Buffer
Overflow

SUMMARY

" <<http://www3.ca.com/Solutions/Product.asp?ID=4536>> BrightStor ARCserve Backup for Windows delivers leading backup and restore protection for all Windows server systems as well as Windows, Linux, Mac OS X and UNIX client environments."

Improper bound checking allows attackers to cause a buffer overflow in Computer Associates BrightStor ARCserve/Enterprise Backup Agents and execute arbitrary code or crash the system.

DETAILS

Vulnerable Systems:

- * BrightStor ARCserve Backup version 11.1
- * BrightStor ARCserve Backup version 11.0
- * BrightStor ARCserve Backup version 9.01
- * BrightStor Enterprise Backup version 10.5
- * BrightStor Enterprise Backup version 10

Securiteam: [NT] Computer Associates BrightStor ARCserve/Enterprise Backup Agents Buffer Overflow

Computer Associates BrightStor ARCserve Backup and BrightStor Enterprise Backup Agents for Windows contain a stack-based buffer overflow vulnerability. The vulnerability may allow remote attackers to execute arbitrary code with SYSTEM privileges, or cause a denial of service condition. The buffer overflow is the result of improper bounds checking performed on data sent to port 6070.

Vendor Status:

The vendor has issued a patch for the vulnerability:

BrightStor ARCserve Backup r11.1 for Windows:

<<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70767&startsearch=1>>
<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70767&startsearch=1>

BrightStor ARCserve Backup r11.0 for Windows:

<<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70769&startsearch=1>>
<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70769&startsearch=1>

BrightStor ARCserve Backup v9.01 for Windows:

<<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70770&startsearch=1>>
<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70770&startsearch=1>

BrightStor Enterprise Backup v10.5 for Windows:

<<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70774&startsearch=1>>
<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70774&startsearch=1>

BrightStor Enterprise Backup v10.0 for Windows:

<<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70773&startsearch=1>>
<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO70773&startsearch=1>

CVE Information:

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

ADDITIONAL INFORMATION

The information has been provided by <<mailto:James.Williams@ca.com>>
Williams, James K.

The original article 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.