

[NT] CA BrightStor ARCserve Backup v11 Discovery Service Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0044.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/13/05

To: list@securiteam.com

Date: 13 Feb 2005 13:43:03 +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 v11 Discovery Service Buffer Overflow

SUMMARY

<<http://www3.ca.com/Solutions/ProductFamily.asp?ID=115>> BrightStor ARCserve Backup for Windows "delivers backup and restore protection for all Windows server systems as well as Windows, Linux, Mac OS X and UNIX client environments".

Remote exploitation of a buffer overflow vulnerability in Computer Associates International Inc's BrightStor ARCserve Backup v11 Discovery Service may allow execution of arbitrary code.

DETAILS

Vulnerable Systems:

* Computer Associates BrightStor ARCserve Backup v11 (Win32)

The BrightStor software will automatically detect other BrightStor (ARCserve) servers on the local network. It does this by sending UDP probe messages to the broadcast address on the network. Each system running the BrightStor software listens for these probes and replies back to IP address embedded in the data of the packet. The Discovery service listens

Securiteam: [NT] CA BrightStor ARCserve Backup v11 Discovery Service Buffer Overflow

on UDP port 41524 for these probe requests.

Analysis:

When a UDP probe is received by the Discovery Service, a stack overflow can occur if the data is larger than the temporary buffer. The `recvfrom()` call made by the service accepts up to 4096 bytes, however the buffer it is copied to is slightly less than 1000 bytes. The return address can be overwritten by sending a message that is at least 967 bytes long. As the service runs as 'Local System', exploitation of this vulnerability allows running arbitrary code with superuser privileges.

Workaround:

Employ firewalls, access control lists or other TCP/UDP restriction mechanism to limit access to systems and services.

Vendor Status:

<<http://supportconnectw.ca.com/public/enews/BrightStor/brigcurrent.asp>>
<http://supportconnectw.ca.com/public/enews/BrightStor/brigcurrent.asp>

The following vendor patches have been made available:

BrightStor ARCserve Backup r11.1 for Windows – All Languages –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62769>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62769>

BrightStor ARCserve Backup r11.0 for Windows – All Languages –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62768>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62768>

BrightStor Enterprise Backup v10.5 for Windows –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62770>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62770>

BrightStor Enterprise Backup v10.0 for Windows –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62771>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62771>

BrightStor ARCserve Backup v9.01 for Windows – All Languages –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62767>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62767>

BrightStor ARCserve 2000 Backup for Windows (Japanese Only) –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62766>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62766>

BrightStor ARCserve Backup r11.1 for NetWare –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62936>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62936>

BrightStor ARCserve Backup v9 for NetWare –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62772>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62772>

Securiteam: [NT] CA BrightStor ARCserve Backup v11 Discovery Service Buffer Overflow

BrightStor ARCserve Backup r11.1 for Windows – 64 Bit Edition –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62990>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62990>

BrightStor ARCserve Backup r11.0 for Windows – 64 Bit Edition –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62989>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62989>

BrightStor Enterprise Backup v10.5 for Windows – 64 Bit Edition –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62991>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62991>

BrightStor ARCserve Backup v9.01 for Windows – 64 Bit Edition –
<<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62987>>
<http://supportconnect.ca.com/sc/redirect.jsp?reqPage=search&searchID=OO62987>

Disclosure Timeline:
11/12/2004 – Initial vendor notification
11/15/2004 – Initial vendor response
02/09/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.
The original article can be found at:
<<http://www.idefense.com/application/poi/display?id=194&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=194&type=vulnerabilities>

=====

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.