

[Full-Disclosure] iDEFENSE Security Advisory 02.10.05: Computer Associates BrightStor ARCserve Backup UniversalAgent Backdoor Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-02/0303.html>

idlabs-advisories_at_idefense.com

Date: 02/10/05

Date: Thu, 10 Feb 2005 14:10:05 -0500

To: <idlabs-advisories@idefense.com>

Computer Associates BrightStor ARCserve Backup UniversalAgent Backdoor
Vulnerability

iDEFENSE Security Advisory 02.10.05

www.idefense.com/application/poi/display?id=198&type=vulnerabilities

February 10, 2005

I. BACKGROUND

BrightStor ARCserve Backup r11.1 delivers leading 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.

II. DESCRIPTION

Remote exploitation of a design flaw in Computer Associates International Inc's BrightStor ARCserve Backup UniversalAgent for UNIX may allow execution of arbitrary code.

The vulnerability specifically exists due to hard coded credentials being left in the production release of the UniversalAgent for UNIX. An attacker may use the following credentials to gain full access to the remote file system and potentially execute arbitrary commands with permissions of the root user.

Username: \x02root\x03

Password: \x02<%j8Uj`~+Ri\x03

III. ANALYSIS

The BrightStor software uses a network agent to perform backups on nodes across the network. Typically, the agent service requires either administrative credentials or a node-specific password and is capable of backing up files and remotely executing commands. The agent will listen on TCP and UDP ports 6051 by default and is installed on every node that the BrightStor server is configured to backup.

IV. DETECTION

Computer Associates BrightStor ARCserve Backup r11.1 for Linux and UNIX have been confirmed vulnerable.

V. WORKAROUND

Employ firewalls, access control lists or other TCP/UDP restriction mechanism to limit access to the backup port on affected systems and services. The login credentials are sent in cleartext and may also be used to detect connections from attackers.

VI. VENDOR RESPONSE

The following vendor advisories are available for this issue:

BAB 7.0 Linux

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63672>

BAB 9.0 Linux Japanese

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63673>

BAB 9.0 Linux English

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63674>

BEB 10.0 AIX

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63675>

BEB 10.0 HPUX

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63676>

BEB 10.0 Solaris

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63677>

BEB 10.5 Tru64

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63678>

BEB 10.5 HP

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63679>

BEB 10.5 AIX

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63680>

BEB 10.5 Solaris

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63681>

BAB 11.1 Macintosh

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63682>

BAB 11.1 Mainframe Linux

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63683>

BAB 11.1 Tru64

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63684>

BAB 11.1 Linux

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63685>

BAB 11.1 HP

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63691>

BAB 11.1 AIX

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63687>

BAB 11.1 – Solaris

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63688>

BEB 10.0 Mainframe Linux

<http://supportconnect.ca.com/sc/solcenter/solresults.jsp?aparno=OO63689>

VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

VIII. DISCLOSURE TIMELINE

12/02/2004 Initial vendor notification

12/02/2004 Initial vendor response

02/10/2005 Coordinated public disclosure

IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research

<http://www.idefense.com/poi/teams/vcp.jsp>

X. LEGAL NOTICES

Copyright (c) 2005 iDEFENSE, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express

written consent of iDEFENSE. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email customerservice@idefense.com for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>