

CA ARCserve Backup for Laptops and Desktops Server LGServer Service Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-08/msg00000.html>

- *From:* "Williams, James K" <James.Williams@xxxxxx>
 - *Date:* Fri, 1 Aug 2008 06:52:07 -0400
-

Title: CA ARCserve Backup for Laptops and Desktops Server LGServer Service Vulnerability

CA Advisory Date: 2008-07-31

Reported By: Vulnerability Research Team of Assurent Secure Technologies, a TELUS Company

Impact: A remote attacker can execute arbitrary code or cause a denial of service condition.

Summary: CA ARCserve Backup for Laptops and Desktops server contains a vulnerability that can allow a remote attacker to execute arbitrary code or cause a denial of service condition. CA has issued updates to address the vulnerability. The vulnerability, CVE-2008-3175, occurs due to insufficient bounds checking by the LGServer service. An attacker can make a request that can result in arbitrary code execution or crash the service.

Mitigating Factors: Only the server installation of BrightStor ARCserve Backup for Laptops and Desktops is affected. The client installation is not affected.

Severity: CA has given this vulnerability a High risk rating.

Affected Products:

CA ARCserve Backup for Laptops and Desktops r11.5
CA ARCserve Backup for Laptops and Desktops r11.1 SP2
CA ARCserve Backup for Laptops and Desktops r11.1 SP1
CA ARCserve Backup for Laptops and Desktops r11.1

CA ARCserve Backup for Laptops and Desktops Server LGServer Service Vulnerability

CA ARCserve Backup for Laptops and Desktops r11.0
CA Desktop Management Suite 11.2
CA Desktop Management Suite 11.1
CA Protection Suites r2
CA Protection Suites 3.0
CA Protection Suites 3.1

Affected Platforms:

Windows

Status and Recommendation:

CA has provided the following updates to address the vulnerability.

CA ARCserve Backup for Laptops and Desktops 11.1, 11.1 SP1, 11.1 SP2:
Upgrade to 11.1 SP2 and apply RO00912.

CA ARCserve Backup for Laptops and Desktops 11.5:
RO00913.

CA Protection Suites 3.0:
RO00912.

CA Protection Suites 3.1:
RO00912.

CA Desktop Management Suite 11.2:
Upgrade to CA Desktop Management Suite 11.2 C1 and apply RO00913.

CA Desktop Management Suite 11.1:
RO01150.

CA ARCserve Backup for Laptops and Desktops 11.0:
Upgrade to ARCserve Backup for Laptops and Desktops version 11.1 SP2 and apply the latest patches.
QI85497.

Note: CA Protection Suites r2 includes CA ARCserve Backup for Laptops and Desktops 11.0.

How to determine if you are affected:

For Windows:

1. Using Windows Explorer, locate the file "rxRPC.dll". The file can be found in the following default locations:

CA ARCserve Backup for Laptops and Desktops 11.5:

CA ARCserve Backup for Laptops and Desktops Server LGServ Service Vulnerability

C:\Program Files\CA\BrightStor ARCserve Backup for Laptops and Desktops\Server

CA ARCserve Backup for Laptops and Desktops 11.1, 11.1 SP1, 11.1 SP2:

C:\Program Files\CA\BrightStor ARCserve Backup for Laptops & Desktops\server

CA Protection Suites 3.0:

C:\Program Files\CA\BrightStor ARCserve Backup for Laptops & Desktops\server

CA Protection Suites 3.1:

C:\Program Files\CA\BrightStor ARCserve Backup for Laptops & Desktops\server

CA Desktop Management Suite 11.2:

C:\Program Files\CA\Unicenter DSM\BABLD\Server

CA Desktop Management Suite 11.1:

C:\Program Files\CA\Unicenter DSM\BABLD\Server

2. Right click on the file and select Properties.

3. Select the General tab.

4. If the file date is earlier than indicated in the below table, the installation is vulnerable.

CA ARCserve Backup for Laptops and Desktops

File Name	File Size (bytes)	File Date
rxRPC.dll	131,072	June 11, 2008

CA ARCserve Backup for Laptops and Desktops 11.1, 11.1 SP1, 11.1 SP2

File Name	File Size (bytes)	File Date
rxRPC.dll	114,688	June 11, 2008

CA Protection Suites 3.0

File Name	File Size (bytes)	File Date
rxRPC.dll	114,688	June 11, 2008

CA Protection Suites 3.1

File Name	File Size (bytes)	File Date
rxRPC.dll	114,688	June 11, 2008

CA Desktop Management Suite 11.2

File Name	File Size (bytes)	File Date
rxRPC.dll	131,072	June 11, 2008

CA Desktop Management Suite 11.1

CA ARCserve Backup for Laptops and Desktops Server LGServer Service Vulnerability

File Name File Size (bytes) File Date
rxRPC.dll 122,880 June 11, 2008

Workaround: None

References (URLs may wrap):

CA Support:

<http://support.ca.com/>

Security Notice for CA ARCserve Backup for Laptops and Desktops
Server LGServer

<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=181721>

Solution Document Reference APARs:

RO00912, RO00913, RO01150, QI85497

CA Security Response Blog posting:

CA ARCserve Backup for Laptops and Desktops Server LGServer
Service Vulnerability

community.ca.com/blogs/casecurityresponseblog/archive/2008/08/01.aspx

Reported By:

Vulnerability Research Team of Assurent Secure Technologies, a
TELUS Company.

<http://www.assurent.com/>

CVE References:

CVE-2008-3175 – LGServer buffer overflow

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3175>

OSVDB References: Pending

<http://osvdb.org/>

Changelog for this advisory:

v1.0 – Initial Release

Customers who require additional information should contact CA
Technical Support at <http://support.ca.com>.

For technical questions or comments related to this advisory,
please send email to vuln AT ca DOT com.

If you discover a vulnerability in CA products, please report your
findings to our product security response team.

<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=177782>

Regards,

Ken Williams ; 0xE2941985

Director, CA Vulnerability Research

CA, 1 CA Plaza, Islandia, NY 11749

Contact <http://www.ca.com/us/contact/>

Legal Notice <http://www.ca.com/us/legal/>

Privacy Policy <http://www.ca.com/us/privacy/>

Copyright (c) 2008 CA. All rights reserved.