

[CAID 35673, 35674, 35675, 35676, 35677]: CA ARCserve Backup for Laptops and Desktops Multiple Server Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-09/msg00273.html>

- *From:* "Williams, James K" <James.Williams@xxxxxx>
 - *Date:* Fri, 21 Sep 2007 14:46:22 -0400
-

Title: [CAID 35673, 35674, 35675, 35676, 35677]: CA ARCserve Backup for Laptops and Desktops Multiple Server Vulnerabilities

CA Vuln ID (CAID): 35673, 35674, 35675, 35676, 35677

CA Advisory Date: 2007-09-20

Reported By: Sean Larsson (VeriSign iDefense Labs)
anonymous researcher working with the iDefense VCP
eEye Digital Security

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

Summary: CA ARCserve Backup for Laptops and Desktops contains multiple vulnerabilities that can allow a remote attacker to cause a denial of service condition or execute arbitrary code. The first set of vulnerabilities, CVE-2007-3216, occur due to insufficient bounds checking on multiple command arguments by the LGServer service. The second set of vulnerabilities, CVE-2007-5003, occur due to insufficient bounds checking on rxrLogin authentication credentials and on a username by the GetUserInfo() function. The third vulnerability, CVE-2007-5004, occurs due to insufficient verification of an integer value used during authentication, which can lead to integer overflow. The fourth vulnerability, CVE-2007-5005, occurs due to insufficient verification of file uploads by the NetBackup service. The fifth vulnerability, CVE-2007-5006, occurs due to insufficient verification of authorization credentials, which can enable an attacker to bypass authentication.

Mitigating Factors:

These issues can only be exploited on a server installation of CA ARCserve Backup for Laptops and Desktops. The client installation

[CAID 35673, 35674, 35675, 35676, 35677]: CA ARCserve Backup for Laptops and Desktops Multiple Server Vulnerabi

is not affected.

Severity: CA has given these vulnerabilities a maximum risk rating of High.

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 r11.0
CA ARCserve Backup for Laptops and Desktops r4.0
CA Desktop Management Suite 11.2
CA Desktop Management Suite 11.1
CA Desktop Management Suite 11.0
CA Protection Suites r2

Affected Platforms:

Windows

Status and Recommendation:

CA has provided updates to address the vulnerabilities.

[CAID 35673, 35674, 35675, 35676, 35677]: CA ARCserve Backup for Laptops and Desktops Multiple Serv