



CVE-2007-5004

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2007-5004
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-01 20:17:00 UTC
Updated	2021-04-08 13:31:00 UTC
Description	Integer overflow in CA (Computer Associates) BrightStor ARCserve Backup for Laptops and Desktops r11.0 through r11.5

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Brightstor Arcserve Backup Laptops Desktops	11.0	All	All	All
Application	Broadcom	Brightstor Arcserve Backup Laptops Desktops	11.1	All	All	All
Application	Broadcom	Brightstor Arcserve Backup Laptops Desktops	11.1	sp1	All	All
Application	Broadcom	Brightstor Arcserve Backup Laptops Desktops	11.5	All	All	All
Application	Broadcom	Brightstor Arcserve Backup Laptops Desktops	4.0	All	All	All
Application	Broadcom	Desktop Management Suite	11.0	All	All	All
Application	Broadcom	Desktop Management Suite	11.1	All	All	All
Application	Broadcom	Desktop Management Suite	11.2	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.0	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.1	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.1	sp1	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.5	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	4.0	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.0	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.1	All	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.1	sp1	All	All
Application	Ca	Brightstor Arcserve Backup Laptops Desktops	11.5	All	All	All

Application	Ca	Brightstor Arcserve Backup Laptops Desktops	4.0	All	All	All
Application	Ca	Desktop Management Suite	11.0	All	All	All
Application	Ca	Desktop Management Suite	11.1	All	All	All
Application	Ca	Desktop Management Suite	11.2	All	All	All
Application	Ca	Desktop Management Suite	11.0	All	All	All
Application	Ca	Desktop Management Suite	11.1	All	All	All
Application	Ca	Desktop Management Suite	11.2	All	All	All
Application	Ca	Protection Suites	r2	All	All	All
Application	Ca	Protection Suites	r2	All	All	All

References

Reference	Source	L
SecurityFocus	BUGTRAQ	w
Resources BeyondTrust	EEYE	re
CA ARCserve Backup for Laptops & Desktops integer overflow vulnerability - CA	CONFIRM	w
SecurityTracker: CA ARCserve Bugs Let Remote Users Execute Arbitrary Code, Bypass Authentication, and Deny Service	SECTRAK	w
CA ARCserve Backup for Laptops & Desktops Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	s
Computer Associates ARCserve Backup Multiple Remote Buffer Overflow Vulnerabilities	BID	w
CA ARCserve Backup for Laptops and Desktops Multiple Server Vulnerabilities - CA	CONFIRM	w
supportconnectw.ca.com/public/sams/lifeguard/infodocs/caarcservebld-securitynotice.asp	CONFIRM	s
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)