CVE-2007-5330

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-5330
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-13 00:17:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The cadbd RPC service in CA BrightStor ARCServe BackUp v9.01 through R11.5, and Enterprise Backup r10.5, allows ren

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-119 | CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Brightstor Arcserve Backup	10.5	All	All	All

Application	Broadcom	Brightstor Arcserve Backup	11	All	All	All
Application	Broadcom	Brightstor Arcserve Backup	11.1	All	All	All
Application	Broadcom	Brightstor Arcserve Backup	11.5	All	All	All
Application	Broadcom	Brightstor Arcserve Backup	9.01	All	All	All
Application	Broadcom	Brightstor Enterprise Backup	10.5	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Computer Associates BrightStor ARCserve Backup Multiple Remote Vulnerabilities
CA BrightStor ARCserve Backup RPC Argument Parsing Vulnerabilities - Secunia Research - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
CA BrightStor ARCServe Backup Multiple Vulnerabilities - Advisories - Secunia
supportconnectw.ca.com/public/storage/infodocs/basb-secnotice.asp
osvdb.org/41373
osvdb.org/41374
IBM X-Force Exchange
SecurityTracker.com Archives - CA BrightStor ARCserve Backup Buffer Overflows and Memory Corruption Errors Let Remote Users Execute
SecurityFocus
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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