



# CVE-2007-0816

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-0816
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-02-07 11:28:00 UTC
<b>Updated</b>	2021-04-07 18:14:00 UTC
<b>Description</b>	The RPC Server service (catirpc.exe) in CA (formerly Computer Associates) BrightStor ARCserve Backup 11.5 SP2 and ea

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	11.5	sp1	All	All
Application	Broadcom	Brightstor Arcserve Backup	11.5	sp2	All	All
Application	Ca	Brightstor Arcserve Backup	11	All	All	All
Application	Ca	Brightstor Arcserve Backup	11.1	All	All	All
Application	Ca	Brightstor Arcserve Backup	11.5	All	All	All
Application	Ca	Brightstor Arcserve Backup	11.5	sp1	All	All
Application	Ca	Brightstor Arcserve Backup	11.5	sp2	All	All
Application	Ca	Brightstor Arcserve Backup	11	All	All	All
Application	Ca	Brightstor Arcserve Backup	11.1	All	All	All
Application	Ca	Brightstor Arcserve Backup	11.5	All	All	All
Application	Ca	Brightstor Arcserve Backup	11.5	sp1	All	All
Application	Ca	Brightstor Arcserve Backup	11.5	sp2	All	All

## References

Reference	Source	Link
CA BrightStor ARCserve Backup RPC Server service (catirpc.exe) denial of service vulnerability - CA	CONFIRM	<a href="http://www3.ca.com">www3.ca.com</a>
CA BrightStor ARCserve Backup Tape Engine and Portmapper Vulnerabilities - CA	CONFIRM	<a href="http://www3.ca.com">www3.ca.com</a>
<a href="http://supportconnectw.ca.com/public/storage/infodocs/babtapeng-securitynotice.asp">supportconnectw.ca.com/public/storage/infodocs/babtapeng-securitynotice.asp</a>	CONFIRM	<a href="http://supportconnectw.ca.com">supportconnectw.ca.com</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
CA BrightStor ARCserve Backup Vulnerabilities - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
32989	OSVDB	<a href="http://osvdb.org">osvdb.org</a>
Computer Associates BrightStor ARCserve Backup Catirpc.EXE Denial Of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
CA BrightStor ARCserve 11.5.2.0 (catirpc.dll) RPC Server DoS Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>
CA BrightStor ARCserve Backup RPC Server Denial of Service - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**