



# CVE-2007-1785

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2007-1785
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-03-31 01:19:00 UTC
<b>Updated</b>	2021-04-07 18:14:00 UTC
<b>Description</b>	The RPC service in mediasvr.exe in CA BrightStor ARCserve Backup 11.5 SP2 build 4237 allows remote attackers to exec

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Broadcom</a>	<a href="#">Brightstor Arcserve Backup</a>	11.1	All	All	All
Application	<a href="#">Broadcom</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	All	All	All
Application	<a href="#">Broadcom</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	sp1	All	All
Application	<a href="#">Broadcom</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	sp2	All	All
Application	<a href="#">Broadcom</a>	<a href="#">Brightstor Arcserve Backup</a>	9.01	All	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11	All	windows	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11.1	All	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	All	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	sp1	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	sp2	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	9.01	All	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11	All	windows	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11.1	All	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	All	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	sp1	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	11.5	sp2	All	All
Application	<a href="#">Ca</a>	<a href="#">Brightstor Arcserve Backup</a>	9.01	All	All	All

## References

Reference	Source	Link
CA BrightStor Backup Buffer Overflow in Mediasvr.exe Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">www.se</a>
SecurityFocus	BUGTRAQ	<a href="#">www.se</a>
Computer Associates BrightStor ARCserve Backup MediaSVR.EXE 191 Buffer Overflow Vulnerability	BID	<a href="#">www.se</a>
CA BrightStor ARCserve Backup MEDIASVR.EXE RPC Request Code Execution - Advisories - Secunia	SECUNIA	<a href="#">secunia</a>
IBM X-Force Exchange	XF	<a href="#">exchan</a>
<a href="#">www.shirkdog.us/camediasvrremote.py</a>	MISC	<a href="#">www.sh</a>
CXSecurity - IDS	SREASON	<a href="#">security</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.vu</a>
<a href="#">supportconnectw.ca.com/public/storage/infodocs/babmedser-secnotice.asp</a>	CONFIRM	<a href="#">support</a>
SecurityFocus	BUGTRAQ	<a href="#">www.se</a>
20070329 CA Brightstor Backup Mediasvr.exe Remote Code Vulnerability	FULLDISC	<a href="#">archive:</a>
<a href="#">www.shirkdog.us/shk-004.html</a>	MISC	<a href="#">www.sh</a>
US-CERT Vulnerability Notes	CERT-VN	<a href="#">www.kc</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist</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](#) 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](#)