



# CVE-2007-0672

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

## Summary

<b>CVE</b>	CVE-2007-0672
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-02-03 01:28:00 UTC
<b>Updated</b>	2021-04-08 13:31:00 UTC
<b>Description</b>	LGSERVER.EXE in BrightStor Mobile Backup 4.0 allows remote attackers to cause a denial of service (disk consumption a

## 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 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	Business Protection Suite	2.0	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 Protection Suite	2.0	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	11.0	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	Business Protection Suite	2.0	All	All	All
Application	Ca	Business Protection Suite	2.0	All	microsoft_sbs_premium	All
Application	Ca	Business Protection Suite	2.0	All	microsoft_sbs_standard	All
Application	Ca	Business Protection Suite	2.0	All	All	All

Application	Ca	<a href="#">Business Protection Suite</a>	2.0	All	microsoft_sbs_premium	All
Application	Ca	<a href="#">Business Protection Suite</a>	2.0	All	microsoft_sbs_standard	All
Application	Ca	<a href="#">Desktop Management Suite</a>	11.0	All	All	All
Application	Ca	<a href="#">Desktop Management Suite</a>	11.1	All	All	All
Application	Ca	<a href="#">Desktop Management Suite</a>	11.0	All	All	All
Application	Ca	<a href="#">Desktop Management Suite</a>	11.1	All	All	All
Application	Ca	<a href="#">Desktop Protection Suite</a>	2.0	All	All	All
Application	Ca	<a href="#">Desktop Protection Suite</a>	2.0	All	All	All

## References

Reference	Source	Link
<a href="https://supportconnectw.ca.com/public/sams/lifeguard/infodocs/babldimpsec-notice.asp">supportconnectw.ca.com/public/sams/lifeguard/infodocs/babldimpsec-notice.asp</a>	CONFIRM	<a href="https://supportconnectw.ca.com">supportconnectw.ca.com</a>
SecurityFocus	BUGTRAQ	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
Computer Associates BrightStor ARCserve Backup LGSERVER.EXE Denial Of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://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](#) 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](https://status.cve.report)