



# CVE-2007-0168

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2007-0168   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2007-01-11 22:28:00 UTC   |
| <b>Updated</b>         | 2021-04-07 18:53:00 UTC   |
| <b>Description</b>     | The Tape Engine service in Computer Associates (CA) BrightStor ARCserve Backup 9.01 through 11.5, Enterprise Backup |

## 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>   | 9.01    | All    | All     | All      |
| Application | <a href="#">Broadcom</a> | <a href="#">Brightstor Arcserve Backup</a>   | All     | All    | All     | All      |
| Application | <a href="#">Broadcom</a> | <a href="#">Brightstor Enterprise Backup</a> | 10.5    | All    | All     | All      |
| Application | <a href="#">Broadcom</a> | <a href="#">Business Protection Suite</a>    | 2.0     | All    | 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>   | 9.01    | All    | All     | All      |
| Application | <a href="#">Ca</a>       | <a href="#">Brightstor Arcserve Backup</a>   | All     | All    | All     | All      |
| Application | <a href="#">Ca</a>       | <a href="#">Brightstor Enterprise Backup</a> | 10.5    | All    | All     | All      |
| Application | <a href="#">Ca</a>       | <a href="#">Brightstor Enterprise Backup</a> | 10.5    | All    | All     | All      |
| Application | <a href="#">Ca</a>       | <a href="#">Business Protection Suite</a>    | 2.0     | All    | All     | All      |
| Application | <a href="#">Ca</a>       | <a href="#">Business Protection Suite</a>    | 2.0     | All    | All     | All      |

## References

| Reference  |
|--|
| <a href="#">Computer Associates BrightStor ARCServe BackUp Tape Engine Remote Code Execution Vulnerability</a> |
| <a href="#">IBM X-Force Exchange</a>   |
| <a href="#">www.lssec.com/advisories/LS-20061002.pdf</a>   |

[livesploit.com/advisories/LS-20061002.pdf](https://livesploit.com/advisories/LS-20061002.pdf)

SecurityFocus

CA BrightStor ARCserve Backup Multiple Vulnerabilities - Advisories - Secunia

ZDI-07-002

[supportconnectw.ca.com/public/storage/infodocs/babimpsec-notice.asp](https://supportconnectw.ca.com/public/storage/infodocs/babimpsec-notice.asp)

SecurityTracker.com Archives - BrightStor ARCserve Backup Bugs in Tape Engine, Mediasvr, and ASCORE.DLL Let Remote Users Execute .

US-CERT Vulnerability Note VU#662400

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

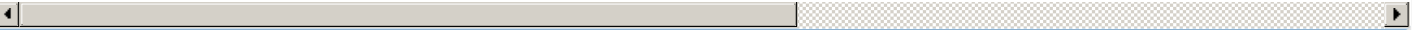
SecurityFocus

SecurityFocus

31327

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.

© [CVE.report](https://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.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

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