



CVE-2007-2863

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

Summary

CVE	CVE-2007-2863
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-06-06 21:30:00 UTC
Updated	2021-04-08 13:07:00 UTC
Description	Stack-based buffer overflow in the Anti-Virus engine before content update 30.6 in multiple CA (formerly Computer Associa

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Anti-virus For The Enterprise	8	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
Application	Broadcom	Common Services	1.0	All	All	All
Application	Broadcom	Common Services	1.1	All	All	All
Application	Broadcom	Common Services	2.0	All	All	All
Application	Broadcom	Common Services	2.1	All	All	All
Application	Broadcom	Common Services	2.2	All	All	All
Application	Broadcom	Common Services	3.0	All	All	All
Application	Ca	Anti-virus For The Enterprise	8	All	All	All
Application	Ca	Anti-virus For The Enterprise	8	All	enterprise	All
Application	Ca	Anti-virus For The Enterprise	8	All	All	All
Application	Ca	Anti-virus For The Enterprise	8	All	enterprise	All
Application	Ca	Brightstor Arcserve Backup	11	All	windows	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	9.01	All	All	All
Application	Ca	Brightstor Arcserve Backup	11	All	windows	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	9.01	All	All	All
Application	Ca	Brightstor Enterprise Backup	10.5	All	All	All
Application	Ca	Brightstor Enterprise Backup	10.5	All	All	All
Application	Ca	Common Services	1.0	All	All	All
Application	Ca	Common Services	1.1	All	All	All
Application	Ca	Common Services	2.0	All	All	All
Application	Ca	Common Services	2.1	All	All	All
Application	Ca	Common Services	2.2	All	All	All
Application	Ca	Common Services	3.0	All	All	All
Application	Ca	Common Services	1.0	All	All	All
Application	Ca	Common Services	1.1	All	All	All
Application	Ca	Common Services	2.0	All	All	All
Application	Ca	Common Services	2.1	All	All	All
Application	Ca	Common Services	2.2	All	All	All
Application	Ca	Common Services	3.0	All	All	All

References

Reference

ZDI-07-034

US-CERT Vulnerability Note VU#739409

35244

supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-securitynotice.asp

IBM X-Force Exchange

SecurityTracker.com Archives - CA Antivirus Stack Overflows in Processing Filenames and the 'coffFiles' Parameter in CAB Files Lets Remote

CA Anti-Virus Engine CAB Archive Processing Buffer Overflows - Advisories - Secunia

Computer Associates Anti-Virus Engine Malformed CAB Filename Buffer Overflow Vulnerability

SecurityFocus

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

CA Multiple Product AV Engine CAB Filename PSO - CXSecurity.com

SecurityFocus

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](#)