



# CVE-2007-4620

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

## Summary

<b>CVE</b>	CVE-2007-4620
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-04-07 18:44:00 UTC
<b>Updated</b>	2021-04-07 18:14:00 UTC
<b>Description</b>	Multiple stack-based buffer overflows in Computer Associates (CA) Alert Notification Service (Alert.exe) 8.1.586.0, 8.0.450.

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	<a href="#">Anti-virus For The Enterprise</a>	7.1	All	All	All
Application	Broadcom	<a href="#">Anti-virus For The Enterprise</a>	8	All	All	All
Application	Broadcom	<a href="#">Anti-virus For The Enterprise</a>	8.1	All	All	All
Application	Broadcom	<a href="#">Brightstor Arcserve Backup</a>	11.1	All	All	All
Application	Broadcom	<a href="#">Brightstor Arcserve Backup</a>	11.5	All	All	All
Application	Ca	<a href="#">Anti-virus For The Enterprise</a>	7.1	All	All	All
Application	Ca	<a href="#">Anti-virus For The Enterprise</a>	8	All	All	All
Application	Ca	<a href="#">Anti-virus For The Enterprise</a>	8.1	All	All	All
Application	Ca	<a href="#">Anti-virus For The Enterprise</a>	7.1	All	All	All
Application	Ca	<a href="#">Anti-virus For The Enterprise</a>	8	All	All	All
Application	Ca	<a href="#">Anti-virus For The Enterprise</a>	8.1	All	All	All
Application	Ca	<a href="#">Brightstor Arcserve Backup</a>	11	All	windows	All
Application	Ca	<a href="#">Brightstor Arcserve Backup</a>	11.1	All	All	All
Application	Ca	<a href="#">Brightstor Arcserve Backup</a>	11.5	All	All	All
Application	Ca	<a href="#">Brightstor Arcserve Backup</a>	11	All	windows	All
Application	Ca	<a href="#">Brightstor Arcserve Backup</a>	11.1	All	All	All
Application	Ca	<a href="#">Brightstor Arcserve Backup</a>	11.5	All	All	All

Application	Ca	<a href="#">Threat Manager For The Enterprise</a>	r8	All	All	All
Application	Ca	<a href="#">Threat Manager For The Enterprise</a>	r8.1	All	All	All
Application	Ca	<a href="#">Threat Manager For The Enterprise</a>	r8	All	All	All
Application	Ca	<a href="#">Threat Manager For The Enterprise</a>	r8.1	All	All	All

## References

### Reference

SecurityFocus

Webmail - OVH

CA Products Alert Notification Server Multiple Vulnerabilities - Advisories - Secunia

SecurityReason - CA Alert Notification Server Multiple Vulnerabilities

CA Threat Manager Buffer Overflows in 'Alert.exe' Let Remote Authenticated Users Execute Arbitrary Code - SecurityTracker

SecurityTracker.com Archives - BrightStor ARCserve Backup Buffer Overflows in 'Alert.exe' Let Remote Authenticated Users Execute Arbitrar

IBM X-Force Exchange

Computer Associates Alert Notification Server Multiple Remote Buffer Overflow Vulnerabilities

404 Not Found

20080403 Computer Associates Alert Notification Service Multiple RPC Buffer Overflow Vulnerabilities

CA Alert Notification Server Multiple Vulnerabilities - CA Security Response Blog - CA

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](#) 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](#)