

# [NEWS] CA Multiple Product AV Engine CAB Header Parsing Stack Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-06/msg00007.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 6 Jun 2007 17:11:39 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

CA Multiple Product AV Engine CAB Header Parsing Stack Overflow  
Vulnerability

---

## SUMMARY

Two vulnerabilities exist that can allow a remote attacker to cause a denial of service or possibly execute arbitrary code. In both instances, an attacker can cause a crash or possibly execute arbitrary code.

## DETAILS

### Affected Products:

- \* CA Anti-Virus for the Enterprise (formerly eTrust Antivirus) r8, r8.1
- \* CA Anti-Virus 2007 (v8)
- \* eTrust EZ Antivirus r7, r6.1
- \* CA Internet Security Suite 2007 (v3)
- \* eTrust Internet Security Suite r1, r2
- \* eTrust EZ Armor r1, r2, r3.x
- \* CA Threat Manager for the Enterprise (formerly eTrust Integrated Threat Management) r8
- \* CA Protection Suites r2, r3
- \* CA Secure Content Manager (formerly eTrust Secure Content Manager) 8.0
- \* CA Anti-Virus Gateway (formerly eTrust Antivirus eTrust Antivirus)

## [NEWS] CA Multiple Product AV Engine CAB Header Parsing Stack Overflow Vulnerability

Gateway) 7.1

- \* Unicenter Network and Systems Management (NSM) r3.0
- \* Unicenter Network and Systems Management (NSM) r3.1
- \* Unicenter Network and Systems Management (NSM) r11
- \* Unicenter Network and Systems Management (NSM) r11.1
- \* BrightStor ARCserve Backup r11.5
- \* BrightStor ARCserve Backup r11.1
- \* BrightStor ARCserve Backup r11 for Windows
- \* BrightStor Enterprise Backup r10.5
- \* BrightStor ARCserve Backup v9.01
- \* CA Common Services
- \* CA Anti-Virus SDK (formerly eTrust Anti-Virus SDK)

The specific flaw exists within the processing of an improperly defined "coffFiles" field in .CAB archives. Large values result in an unbounded data copy operation which can result in an exploitable stack-based buffer overflow.

Vendor Status:

Computer Associates has issued an update to correct this vulnerability. More details can be found at:

<http://supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-securitynotice.asp>  
<http://supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-securitynotice.asp>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2864>  
CVE-2007-2864

Disclosure Timeline:

- \* 2007.02.16 – Vulnerability reported to vendor
- \* 2007.06.05 – Coordinated public release of advisory

### ADDITIONAL INFORMATION

The information has been provided by ZDI-07-035.

The original article can be found at:

<http://www.zerodayinitiative.com/advisories/ZDI-07-035.html>  
<http://www.zerodayinitiative.com/advisories/ZDI-07-035.html>

Related article can be found at:

<http://supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-securitynotice.asp>  
<http://supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-securitynotice.asp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

[NEWS] CA Multiple Product AV Engine CAB Header Parsing Stack Overflow Vulnerability

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.