

[NT] CA Anti-Virus vetfddnt.sys and vetmonnt.sys Local DoS Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00043.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2006 17:04:16 +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 Anti-Virus vetfddnt.sys and vetmonnt.sys Local DoS Vulnerabilities

SUMMARY

Multiple instances of improper handling of NULL buffers in CA Anti-Virus allow local attackers to cause a denial of service condition. This issue affects only consumer CA Anti-Virus products.

DETAILS

Vulnerable Systems:

- * CA Anti-Virus 2007 version 8.1
- * CA Anti-Virus for Vista Beta version 8.2
- * CA Internet Security Suite 2007 version 3.0

Status and Recommendation:

CA has addressed this issue in the GA (Generally Available) software by providing a new automatic update on December 13, 2006. Customers running one of the GA products simply need to ensure that they have allowed this automatic update to take place. For CA Anti-Virus for Vista Beta, this issue will be patched in the GA release of the software.

Determining if you are affected:

[NT] CA Anti-Virus vetfddnt.sys and vetmonnt.sys Local DoS Vulnerabilities

View the Help>About screen and confirm that the product version is 8.3.0.1 or above. You can also verify application of the update by confirming that the vetfddnt.sys and vetmonnt.sys driver versions are 8.3.0.1 or above. These files are located in the %windows%\system32\drivers folder.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6496>>
CVE-2006-6496

ADDITIONAL INFORMATION

The information has been provided by <<mailto:James.Williams@xxxxxx>>
Williams, James K.

The original article can be found at:

<<http://www3.ca.com/securityadvisor/newsinfo/collateral.aspx?cid=96883>>
<http://www3.ca.com/securityadvisor/newsinfo/collateral.aspx?cid=96883>

=====

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

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

list-unsubscribe@xxxxxxxxxxxxxx

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

=====

=====

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.