

# [NT] Symantec AntiVirus and Symantec Client Security Elevation of Privilege

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00026.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 20 Sep 2006 16:50:24 +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>

-----

Symantec AntiVirus and Symantec Client Security Elevation of Privilege

---

## SUMMARY

An elevation of privilege vulnerability in Symantec Client Security and Symantec AntiVirus Corporate Edition could potentially allow a local attacker to execute code with elevated privileges on the target machine.

## DETAILS

### Affected Products:

- \* Symantec AntiVirus Corporate Edition versions 10.0, 9.x, and 8.1
- \* Symantec Client Security versions 3.0, 2.x, 1.x

### Unaffected Products:

- \* Symantec AntiVirus Corporate Edition version 10.1
- \* Symantec Client Security version 3.1

Deral Heiland of Layered Defense notified Symantec of a format string vulnerability within Symantec AntiVirus Corporate Edition. If successfully exploited, the vulnerability could allow a local attacker to execute code with elevated privileges on the local system.

[NT] Symantec AntiVirus and Symantec Client Security Elevation of Privilege

In addition, Symantec engineers found a second format string vulnerability in the alert notification process. This issue could allow a local user to replace the alert notification message with a format string which could cause potentially cause the Real Time Virus Scan service to crash when the notification message is displayed following the detection of a malicious file.

Symantec Response:

Symantec engineers have verified that these vulnerabilities exist in the product versions indicated, and have provided updates to address the issue.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3454>>  
CVE-2006-3454

ADDITIONAL INFORMATION

The information has been provided by <<mailto:secure@xxxxxxxxxxxxx>>  
Symantec Security.

The original article can be found at:

<<http://www.symantec.com/avcenter/security/Content/2006.09.13.html>>  
<http://www.symantec.com/avcenter/security/Content/2006.09.13.html>

=====

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@xxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxx)

=====  
=====

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.