

# [NT] Stack Overflow in 3rd Party ActiveX Controls affects Multiple Vendor Products

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00048.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 30 Apr 2007 19:39:38 +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>

-----

Stack Overflow in 3rd Party ActiveX Controls affects Multiple Vendor Products

---

## SUMMARY

Vulnerabilities were identified in third-party trouble-shooting ActiveX controls, developed by SupportSoft. Two of these controls were signed, shipped and installed with the identified versions of Symantec's consumer products and as part of the Symantec Automated Support Assistant support tool. The vulnerability identified in the Symantec shipped controls could potentially result in a stack overflow requiring user interaction to exploit. If successfully exploited this vulnerability could potentially compromise a user's system possibly allowing execution of arbitrary code or unauthorized access to system assets with the permissions of the user's browser.

## DETAILS

Vulnerable Systems:

- \* Symantec Automated Support Assistant
- \* Symantec Norton AntiVirus 2006
- \* Symantec Norton Internet Security 2006
- \* Symantec Norton System Works 2006

## [NT] Stack Overflow in 3rd Party ActiveX Controls affects Multiple Vendor Products

### Immune Systems:

- \* Symantec 2007 Consumer Products
- \* Symantec Norton 360
- \* Symantec Corporate and Enterprise Products

Symantec was initially alerted by Next Generation Security Software (NGSS), to stack overflow and unauthorized access vulnerabilities identified in two SupportSoft ActiveX controls, SmartIssue tgctlsi.dll and ScriptRunner tgctlsr.dll, that Symantec signed and shipped with some of Symantec's 2006 consumer products and used by the Symantec Automated Support Assistant support tool Symantec provides on its consumer support site.

These SupportSoft ActiveX components did not properly validate external input. This failure could potentially lead to unauthorized access to system resources or the possible execution of malicious code with the privileges of the user's browser, resulting in a potential compromise of the user's system.

Any attempt to exploit these issues would require interactive user involvement. An attacker would need to be able to effectively entice a user to visit a malicious web site where their malicious code was hosted or to click on a malicious URL in any attempt to compromise the user's system. While these SupportSoft-developed components should also have been effectively site-locked, which would have further reduced the severity, this capability was found to be improperly implemented in the vulnerable versions.

### Symantec Response:

Symantec worked closely with SupportSoft to ensure updates were quickly made available for the identified controls. SupportSoft has posted a Security Bulletin,

<[http://www.supportsoft.com/support/controls\\_update.asp](http://www.supportsoft.com/support/controls_update.asp)>  
[http://www.supportsoft.com/support/controls\\_update.asp](http://www.supportsoft.com/support/controls_update.asp), for the controls Symantec uses and controls used in other products on their support site, [www.supportsoft.com](http://www.supportsoft.com).

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6490>>  
CVE-2006-6490

### 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/2007.02.22.html>>  
<http://www.symantec.com/avcenter/security/Content/2007.02.22.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@xxxxxxxxxxxxxxxxx

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

=====

=====

**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.