

# [NT] Buffer Overrun in TSAC ActiveX Control Could Allow Code Execution

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0090.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/25/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sun, 25 Aug 2002 19:07:02 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Buffer Overrun in TSAC ActiveX Control Could Allow Code Execution

---

## SUMMARY

The Terminal Services Advanced Client (TSAC) web control is an ActiveX control that can be used to run Terminal Services sessions within Internet Explorer. The downloadable ActiveX control provides nearly the same functionality as the full Terminal Services Client, but is designed to deliver this functionality over the Web.

The TSAC control does not come installed as part of any Windows client system. Instead, clients obtain the control from web servers that offer terminal services. The configuration process that enables an IIS server to provide terminal services involves installing on the server a cabinet file containing the control. The server then delivers the cabinet file to any client system that needs it, and the client installs the control via the cabinet file.

A security vulnerability results because the control contains an unchecked buffer in the code that processes one of the input parameters. By calling the control on a client system and overrunning the buffer, an attacker could gain the ability to run code in the security context of the currently logged on user. This would enable the attacker to take any desired action on the user's system. The attacker could mount an attack by

## Securiteam: [NT] Buffer Overrun in TSAC ActiveX Control Could Allow Code Execution

either hosting a web page that exploits the vulnerability against any user who visits it, or by sending an HTML mail to another user.

### DETAILS

#### Affected Software:

\* Microsoft Terminal Services Advanced Client (TSAC) ActiveX control, which can be installed on any Windows system.

#### Mitigating factors:

\* The vulnerability could only be exploited if the TSAC control had been installed on the user's system by an IIS server hosting the control.

\* The vulnerability poses no threat to servers that host it. While housed on the server, the control is encapsulated in a cabinet file and cannot be executed.

\* The HTML mail-based attack vector could not be exploited on systems where Outlook 98 or Outlook 2000 were used in conjunction with the Outlook Email Security Update, or Outlook Express 6 or Outlook 2002 were used in their default configurations

#### Patch availability:

##### Download locations for this patch

\* Web masters whose sites offer terminal services should install the patch at:

<<http://www.microsoft.com/windowsxp/pro/downloads/rdwebconn.asp>>  
<http://www.microsoft.com/windowsxp/pro/downloads/rdwebconn.asp>

\* Customers should install the latest IE cumulative patch. At this writing, the latest IE patch is available in Microsoft Security Bulletin <<http://www.microsoft.com/technet/security/bulletin/MS02-047.asp>> MS02-047.

#### What is the scope of the vulnerability?

This is a buffer-overrun vulnerability. An attacker could exploit the vulnerability via either a web page or an HTML mail, and successfully exploiting it would grant the attacker complete control over a user's system. This would give the attacker the ability to add, delete or change any data on the system, reformat the hard drive, or take other actions.

#### The vulnerability is subject to several constraints:

\* The vulnerability could only be exploited if the control were installed on the user's system. However, it is not installed by default as part of any version of Windows.

\* Customers who use Outlook 98 or Outlook 2000 in conjunction with the Outlook Email Security Update, or who use Outlook Express 6 or Outlook 2002, would be at no risk from the email-based attack vector.

#### What causes the vulnerability?

The vulnerability results because the Terminal Services Advanced Client (TSAC) ActiveX control contains an unchecked buffer. If called by a web site in a particular way, the buffer could be overrun, with the result that an attacker could cause the control to take action on the user's

system.

What is the TSAC ActiveX control?

The Terminal Services Advanced Client (TSAC) ActiveX provides a way for Windows systems to run Terminal Services sessions within Internet Explorer. It provides nearly the same functionality as the full Terminal Services Client, but is designed to deliver this functionality over the Web. Through the control, users can establish terminal server sessions from suitably configured IIS servers.

Is the TSAC control installed by default?

No. In fact, you cannot install the control by any means except visiting a web site that offers terminal services. The control is downloaded from the server to the client system as part of the session connection sequence.

How does the installation process for the TSAC control work?

By default, IIS web sites do not offer access to terminal services enabled machines. When an administrator chooses to configure the site to provide them, he or she must download a hostable version of the control from the Microsoft web site and install it on the server. (In the case of Windows XP Professional, the hostable version of the control can also be obtained from the installation CD). Once this has been done, the server will download the control to any system that visits the web site, after which point the user can start terminal service sessions with the web site.

Can the control be installed by a web site without the user's knowledge?

No. The installation process always generates a warning to user, and the user does have the opportunity to cancel.

What is wrong with the TSAC ActiveX control?

The control contains an unchecked buffer. If called using a particular type of malformed input value, the buffer could be overrun. The effect would be, in essence, to change the functionality of the control and make it take new actions instead of those it is programmed to take.

What could this vulnerability enable an attacker to do?

An attacker could use this vulnerability to gain control over another user's computer. Depending on exactly how the attacker overran the buffer, he or she could cause the control to take any desired action. Because the control operates in the context of the user, the attacker would be able to perform any action the user was able to perform.

How might an attacker exploit the vulnerability?

The attacker would need to construct a web page that calls the control and provides the malformed input value discussed above. The attack could then proceed via either of two vectors. In the first, the attacker could host the web page on a web site; when a user visited the site, the web page would attempt to run the control and exploit the vulnerability. In the second, the attacker could send the web page as an HTML mail. Upon being opened by the recipient, the web page could attempt to run the control and exploit the vulnerability.

## Securiteam: [NT] Buffer Overrun in TSAC ActiveX Control Could Allow Code Execution

You said the web page could "attempt" to run the control. What would determine whether this attempt was successful?

Two factors would determine whether the attack was successful:

- \* Whether the user had previously accepted the installation of the control from a web site. If the control was not present on the system, it could not be called. As discussed above, the control is not installed by default in any version of Windows.

- \* Whether ActiveX controls were allowed to run on the user's system. The Internet Explorer Security Zones mechanism provides a way of regulating what actions various web sites can take – among them, whether they can run ActiveX controls. By default, web pages in the Restricted Sites Zone cannot run ActiveX controls. This turns out to be especially significant in the case of an attack via the HTML mail vector.

Why is that?

By default, Outlook Express 6.0 and Outlook 2002 open HTML mails in the Restricted Sites Zone. In addition, Outlook 98 and 2000 open HTML mails in the Restricted Sites Zone if the Outlook Email Security Update has been installed. Customers who use any of these products would be at no risk from the email attack vector.

In the Summary section of the bulletin, you recommended that web masters who offer terminal services install the patch. Does that mean this vulnerability poses a threat to my web site?

No. The vulnerability poses a threat to the clients in this scenario, not the server. When hosted on a server, the control is encapsulated in a compressed file (called a cabinet file). It cannot be executed while in this state.

If the vulnerability does not pose a threat to my web site, why do I have to install the new patch on my server?

To be clear, you may not need to install it. Only web sites that provide terminal services and which host the TSAC control need to install the new patch. However, if you do provide terminal services, you should install the patch in order to ensure that your web site is hosting the most up to date version of the control. If you do not, users who take the actions we recommend below will be unable to use access terminal services enabled machines from your web site.

After installing the patch on my web server, do I need to take any other action?

Yes. You will need to follow the instructions in Microsoft Knowledge Base article Q327521 for updating your web pages to use the new control.

In the Summary section of the bulletin, you recommended that users should not install this patch, but instead should install the most recent cumulative patch for IE. Why?

The latest cumulative patch for IE (which, at this writing, is the one provided in Microsoft Security Bulletin MS02-047) sets the "kill bit" for the control. This action in itself is sufficient to protect users from the vulnerability, because it prevents the vulnerable version of the control

## Securiteam: [NT] Buffer Overrun in TSAC ActiveX Control Could Allow Code Execution

from ever being instantiated within Internet Explorer. (For more information on the "kill bit", see Microsoft Knowledge Base article Q240797.

But why aren't you providing an updated control for users to install on their systems?

The updated control will be delivered to users through the normal installation process described above. That is, the next time the user visits a web site that offers terminal services and has installed the patch, the updated control will be delivered to the user's system. (On the other hand, if the web site has not installed the patch, the user will be unable to use terminal services. This is the correct behavior, since the older version of the control does represent a security exposure if used).

I do not know whether I have ever visited a web site that installed the TSAC control. Should I install the latest IE patch?

Yes. The patch provided in Microsoft Security Bulletin MS02-047 contains fixes for a number of vulnerabilities in addition to this one. It is worth installing in its own right, even if you do not have the TSAC control.

How can I tell if the TSAC ActiveX control is already on my computer?

To see if the control is on your computer, do the following:

- 1) Start Internet Explorer
- 2) Select Tools, then Internet Options.
- 3) Click on the General tab.
- 4) Click on Settings, then click on View Objects.
- 5) Search the resulting list for a Program File name called Microsoft Terminal Services Client Control or Microsoft RDP Client Control
- 6) If neither of these files are present, you definitely do not have the TSAC control installed.
- 7) If Microsoft Terminal Service Client Control or Microsoft RDP Client control is present, right-click on it and select properties, then look for one of the following IDs. If either are present, you have a vulnerable version of the TSAC control installed.
  - \* {1fb464c8-09bb-4017-a2f5-eb742f04392f}
  - \* {791fa017-2de3-492e-acc5-53c67a2b94d0}

I do have the vulnerable control on my system, but I do not want to install the IE patch. Is there another way to protect my system?

Yes. You can set the "kill bit" manually. Just follow the instructions in Microsoft Knowledge Base Article Q240797, and set the "killbit" for the following IDs:

- \* {1fb464c8-09bb-4017-a2f5-eb742f04392f}
- \* {791fa017-2de3-492e-acc5-53c67a2b94d0}

My system is set up by my administrator to not install ActiveX controls. What should I do?

You may be part of the Users group, which by default doesn't allow ActiveX controls to be installed. You will need to contact your administrator about how you can install the ActiveX control. The administrator will determine what method will be used in your organization.

Securiteam: [NT] Buffer Overrun in TSAC ActiveX Control Could Allow Code Execution

What does the patch do?

The patch addresses the vulnerability by instituting proper input data checking in the TSAC ActiveX control.

ADDITIONAL INFORMATION

The information has been provided by

[0\\_35557\\_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C\\_US@Newsletters.Microsoft.com](mailto:0_35557_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com)

Microsoft Product Security.

=====

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@securiteam.com](mailto:list-unsubscribe@securiteam.com)

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

=====

=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Unchecked Buffer in Network Share Provider Can Lead to Denial of Service"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)