

[NT] Microsoft Terminal Server Client Buffer Overrun

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0114.html>

From: support@securiteam.com

Date: 08/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 28 Aug 2002 23:49:15 +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.

Microsoft Terminal Server Client Buffer Overrun

SUMMARY

<<http://www.microsoft.com/windows2000/downloads/recommended/default.asp>>

Microsoft Terminal Server ActiveX client is the ActiveX version of the standard Windows Terminal Services client. It allows a client to connect to a Terminal Server from a web page. This allows a web developer to integrate a Win32-based application into a web page.

There is a buffer-overrun vulnerability in one of the parameters used by the ActiveX component when it is embedded in a web page. An attacker could exploit this vulnerability to run malicious code on a target system. The user would need to open a malicious HTML file as an attachment to an email message, as a file on the local or network file system or as a link on a malicious web site. If the malicious HTML file is opened, it will cause the Active X component to execute the arbitrary computer code contained within the HTML page with the permissions of the attacker.

Since the Microsoft Terminal Server ActiveX client is signed by Microsoft and marked safe there is no warning with the default Internet Explorer security settings if you have previously selected to trust all controls signed by Microsoft. This is a good example of why not to trust any ActiveX components from an unknown source. A malicious site could use an

Securiteam: [NT] Microsoft Terminal Server Client Buffer Overrun

old vulnerable version of the ActiveX control even after the patched ActiveX component is available from Microsoft. If users install the latest vendor, cumulative patch for Internet Explorer this problem is eliminated.

DETAILS

Vulnerable systems:

* Microsoft Terminal Server ActiveX Client v5.02221.1

By default the Terminal Server ActiveX client will install itself in a directory such as '<http://site/tsweb/>'. The buffer-overflow condition occurs when a large string is used for the server name field. We were able to cause an exception to occur with a long string made up of the letter 'A'. The result was the over writing of EIP with 0x41414141. ESI will point the buffer of supplied data.

The ID of the component tested was: 1FB464C8-09BB-4017-A2F5-EB742F04392F

Vendor Response:

Vendor has bulletin and patch for Terminal Server

<<http://www.microsoft.com/technet/security/bulletin/ms02-046.asp>>

<http://www.microsoft.com/technet/security/bulletin/ms02-046.asp>

Vendor has bulletin and patch for Internet Explorer

<<http://www.microsoft.com/technet/security/bulletin/MS02-047.asp>>

<http://www.microsoft.com/technet/security/bulletin/MS02-047.asp>

Recommendation:

You should never open attachments/webpages that come from unknown sources no matter how benign they may appear. Be wary of those that come from known sources.

You should consider the benefits and risks of each attachment file type or ActiveX control that you let into your organization. Attachment file types or ActiveX controls that you do not need should be dropped at your perimeter mail gateway or proxy server. Attachments that you choose to forward on into your organization should be scanned for known malicious code using a antivirus product.

End users should install the latest Internet Explorer cumulative patch that sets the Kill Bit on the vulnerable version of the ActiveX component so it will not execute.

Terminal Server administrators should install the vendor patch to update the ActiveX component they have available for download. Until this patch is installed, users who have installed the Internet Explorer cumulative patch will not be able to access the Terminal Server via the ActiveX component.

ADDITIONAL INFORMATION

Securiteam: [NT] Microsoft Terminal Server Client Buffer Overrun

The information has been provided by <mailto:advisories@atstake.com>
@stake Advisories.

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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: "[UNIX] Linuxconf Locally Exploitable Buffer Overflow Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)