

[NT] Microsoft Internet Explorer % Encoding Security Issue (CSS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0053.html>

From: support@securiteam.com

Date: 09/14/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 14 Sep 2002 19:31:18 +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 Internet Explorer % Encoding Security Issue (CSS)

SUMMARY

A security vulnerability in Internet Explorer allows attackers to cause the product to reveal sensitive cookies of third party sites. This is caused by inconsistent decoding of URL information, causing the domain name that is used by the cookie domain to decode differently from that of the actual domain name being accessed.

DETAILS

Vulnerable systems:

* Internet Explorer version 6.0.2600.0000

%xx values in the URL are decoded when IE calculates the domain, but not decoded while downloading a page. Therefore, if we have a URL such as:

www.yahoo.com%2F@clik.to/liudieyu"><http://www.yahoo.com%2F@clik.to/liudieyu> (where 2F equals to hex\$(asc('/))), the URL will lead to clik.to/liudieyu instead of www.yahoo.com, while the domain as seen by IE is www.yahoo.com.

Demonstration:

A demonstration is available at:

<<http://www16.brinkster.com/liudieyu/2FforMSIE/2FforMSIE-MyPage.htm>>

Securiteam: [NT] Microsoft Internet Explorer % Encoding Security Issue (CSS)

<http://www16.brinkster.com/liudieyu/2FforMSIE/2FforMSIE-MyPage.htm>

Alternatively, it is also available at:

<clik.to/liudieyu> clik.to/liudieyu (going to the 2FforMSIE-MyPage section).

ADDITIONAL INFORMATION

The information has been provided by

<mailto:liudieyuinchina@yahoo.com.cn> Liu Die Yu.

=====

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] ht://Check Cross-Site Scripting"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)