

[NT] Microsoft Internet Explorer about:blank Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0047.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/14/03

To: list@securiteam.com

Date: 14 Aug 2003 15:18:20 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

Microsoft Internet Explorer about:blank Cross Site Scripting

SUMMARY

A Cross Site Scripting vulnerability has been discovered in Internet Explorer's about:blank page. The vulnerability allows attackers to cause the product to execute arbitrary HTML and/or JavaScript.

DETAILS

Vulnerable systems:

- * Internet Explorer version 6.0.2600.x (without SP1)
- * Internet Explorer version 5.0.x
- * Internet Explorer version 4.x
- * Internet Explorer version 3.x

Immune systems:

- * Internet Explorer version 6.0.2600.x with SP1

Securiteam: [NT] Microsoft Internet Explorer about:blank Cross Site Scripting

By passing a specially crafted URL to the Internet Explorer, a remote attacker can cause the product to return arbitrary HTML and/or JavaScript.

Examples:

```
about:blank%20< script>alert('8-D uhh !');</script>  
about:blank%20< iframe src="about:blank%20<h1>;- )" ></iframe>  
about:blank%20< h1>XSS is behind you...</h1>
```

ADDITIONAL INFORMATION

The information has been provided by Lorenzo Hernandez Garcia-Hierro .

=====

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.