

# [NT] Additional Details Released on the Zone Spoofing Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0036.html>

---

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

*Date:* 10/15/01

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

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

Subject: [NT] Additional Details Released on the Zone Spoofing Vulnerability

Message-Id: <20011014223039.BA67F138C1@mail.der-keiler.de>

Date: Mon, 15 Oct 2001 00:30:39 +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.

-----

Additional Details Released on the Zone Spoofing Vulnerability

---

## SUMMARY

Microsoft Internet Explorer security is dependant on different 'security zones'. These zones (Local Intranet zone and Internet zone) can have different security settings in regards to scripting and ActiveX execution. A lot of individuals and companies (including Microsoft) are depending on these zones to allow custom written ActiveX controls (unsigned and unsafe for scripting) to run on their internal intranet or network. A flaw has been discovered in Internet Explorer that can bypass these zones and 'fool' the browser into believing an Internet site resides in the local intranet zone. This has as result that malicious website owners could potentially operate (and execute malicious code) in the users local intranet zone by luring surfers to their site with specially crafted URL's.

In order for this Flaw to be dangerous, the user would have to have lower security settings in the intranet zone then in the Internet zone.

## DETAILS

## Securiteam: [NT] Additional Details Released on the Zone Spoofi

Vulnerable systems:

Microsoft Internet Explorer 4.x

Microsoft Internet Explorer 5.x

Example:

An option in a basic authenticated site is to pass on a username (and/or password) in the URL like this:

[mike@msdn.microsoft.com](http://mike@msdn.microsoft.com)"><http://mike@msdn.microsoft.com>

Another possibility is to convert an IP address into a dotless IP address; such an address is also called a DWORD address (some proxy servers, routers or web servers do not allow this).

<http://msdn.microsoft.com> – IP: 207.46.239.122

Convert this IP address to a DWORD address:

207 \* 16777216 = 3472883712

46 \* 65536 = 3014656

239 \* 256 = 61184

122 \* 1 = 122

----- +  
= 3475959674

This DWORD address can be used to visit the site like:

<http://3475959674>

If we combine the URL login option with the DWORD IP address, we will get the following URL:

<http://mike@3475959674>

The browser still thinks we are in the internet zone as expected.

Now we change the @ sign to its ASCII equivalent (%40):

-----  
<http://mike%403475959674>  
-----

Using this link, the browser thinks the Internet site we are in is the local intranet zone.

Solution:

An official Microsoft patch that will fix this can be found at the following address:

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-051.asp>>  
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-051.asp>

Securiteam: [NT] Additional Details Released on the Zone Spoofi

ADDITIONAL INFORMATION

The information has been provided by <mailto:[unhackables@hotmail.com](mailto:unhackables@hotmail.com)>  
kikkert 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] Ipswitch Web Calendaring Buffer Overflow"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)