

[NT] VisNetic WebSite XSS vulnerability through HTTP Referer header

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0049.html>

From: support@securiteam.com

Date: 12/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: 15 Dec 2002 23:39:02 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

VisNetic WebSite XSS vulnerability through HTTP Referer header

SUMMARY

<http://www.deerfield.com/download/visnetic_website/> VisNetic Website, the first web server developed specifically for Windows, can use almost any development platform, and includes features that allow web developers to create powerful, flexible web sites. VisNetic WebSite is a secure Windows-based web server that supports multiple domains, and allows TLS/SSL secured domains. This web server also includes support for a user database that can restrict access to content, and is immune to many of the security issues that may arise with other popular web servers. A vulnerability in the product allows remote attackers to cause a cross site scripting vulnerability by inserting malicious HTML and/or JavaScript into the HTTP Referer header.

DETAILS

Vulnerable systems:

- * VisNetic WebSite version 3.5.13.1

Immune systems:

- * VisNetic WebSite version 3.5.15

Securiteam: [NT] VisNetic WebSite XSS vulnerability through HTTP Referer header

Impact:

Loss of privacy – user cookies associated with the target site may be stolen in some cases.

Technical details:

VisNetic WebSite server will return a customized 404 page when a requested page does not exist. This customized 404 page contains a link to the last visited web page, and by clicking on the link the user is redirected back to where he/she came from. This link is created by using the data in the HTTP 'Referer' header, which is sent automatically by the web browser. By requesting a non-existent page, and changing the HTTP 'Referer' header to contain malicious JavaScript code, an attacker may force the application to return the JavaScript code to the web browser, where it will be executed.

Example Exploit:

The following request will return a JavaScript pop-up screen:

```
GET /NonExistentPage.html HTTP/1.0
Host: TARGET
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: "></a><scr!pt>alert('Cross Site Scripting')</scr!pt>
```

Fix:

The new version of VisNetic WebSite (3.5.15) solves this problem. You can download it from:

<http://www.deerfield.com/products/visnetic_website/>
http://www.deerfield.com/products/visnetic_website/

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ory.segal@sanctuminc.com>>
Ory Segal.

=====

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.