

[NT] Multiple Vulnerabilities in AspDotNetStorefront

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0030.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 06/10/04

To: list@securiteam.com

Date: 10 Jun 2004 11:37:09 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Multiple Vulnerabilities in AspDotNetStorefront

SUMMARY

<<http://www.aspdotnetstorefront.com/default.aspx>> AspDotNetStorefront is a "complete E-commerce Storefront & Shopping Cart Includes all C# source code & SQL Server database schema". Multiple vulnerabilities in AspDotNetStorefront allow a remote attacker to delete files from the servers, execute uploaded files and perform cross-site-scripting attacks.

DETAILS

Vulnerable Systems:

* AspDotNetStorefront version 3.3. Previous versions may also be affected.

Remote image deletion:

If a malicious user knows a ProductID has the ability to remotely delete the image off the server. The malicious user can do so because deleteicon.aspx in the admin area fails to validate the session.

Example:

<http://example/aspdotnetcart/admin/deleteicon.aspx?ProductID=1&FormImageName=Pic1&size=icon>

Securiteam: [NT] Multiple Vulnerabilities in AspDotNetStorefront

Remote file execution:

If a malicious user brute forces the password for the admin area, he will have the ability to upload and execute any Trojan or malicious code. This can be done because: /aspdotnetcart/admin/images.aspx fails to validate what extensions and/or mime types are allowed to be uploaded.

Cross site scripting:

A malicious user is able to compromise the hidden field ReturnURL to invoke a Cross-Site Scripting attack. This can be used to take advantage of the trust between a client and server allowing the malicious user to execute malicious JavaScript on the client's machine.

Examples:

```
http://www.example.com/aspdotnetcart/admin/signin.aspx?returnurl=1" style="background:url(javascript:alert('Vulnerable_To_XSS'))"%20" http://www.example.com/aspdotnetcart/admin/signin.aspx?returnurl=---> <script>alert('Vulnerable_To_XSS')</script> http://www.example.com/aspdotnetcart/admin/signin.aspx?returnurl=>"> <script>alert("Vulnerable_To_XSS")</script> http://www.example.com/aspdotnetcart/admin/signin.aspx?returnurl=>"> <img%20src="javascript:alert('Vulnerable_To_XSS')">
```

Vendor Status:

Updates are available for customers to download at:

<<http://www.aspdotnetstorefront.com>> <http://www.aspdotnetstorefront.com>

Vendor was provided a list of vulnerabilities on June 5th. Application was fixed by June 6th.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:tommy@providesecurity.com>> Thomas Ryan.

=====

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.