

Securiteam: [NT] 04WebServer Multiple Vulnerabilities (CSS, Log File Injection, AUX DoS)

[NT] 04WebServer Multiple Vulnerabilities (CSS, Log File Injection, AUX DoS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0036.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/15/04

To: list@securiteam.com

Date: 15 Nov 2004 19:33:55 +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>

04WebServer Multiple Vulnerabilities (CSS, Log File Injection, AUX DoS)

SUMMARY

<<http://www.soft3304.net/04WebServer/>> 04WebServer is "a HTTP server developed by Soft3304 for Windows platforms. It is an easy-to-configure personal HTTP server that supports CGI, SSI, WebDAV and SSL/TLS". This advisory documents three vulnerabilities that were found in 04WebServer.

DETAILS

Vulnerable Systems:

* 04WebServer version 1.42

04WebServer is a HTTP server developed by Soft3304 for Windows platforms. It is an easy-to-configure personal HTTP server that supports CGI, SSI, WebDAV and SSL/TLS. This advisory documents three vulnerabilities that were found in version 1.42 of 04WebServer. This includes a XSS vulnerability, lack of character filtering when writing to log file, and potential server restart problem after requesting a DOS device in the URL.

1. Cross-Site Scripting (XSS) Vulnerability in Default Error Page

When the user requests for a non-existing page from the web server, the

Securiteam: [NT] 04WebServer Multiple Vulnerabilities (CSS, Log File Injection, AUX DoS)

default error page Response_default.html will be served out to user. This page displays the user's requested URL without properly escaping HTML special characters. This may be exploited by a malicious user to execute malicious Javascript on the victim's browser, stealing his cookie. The following sample HTTP request demonstrates the XSS vulnerability by displaying a harmless popup dialog box.

Example:

```
http://[hostname]/<script>alert('XSS');</script>
```

2. Lack of Character Filtering allows an Attacker to Inject Arbitrary Characters into Log File

User's HTTP requests are logged into a text file in the \04WebServer142\Logs directory. The server performs only minimally filtering on the request URL before writing it into the log file. This allows the attacker to inject arbitrary characters into the log file. In particular, it may be possible for the attacker to submit specifically crafted HTTP requests that would create fictitious entries in the log. The following HTTP request, when submitted to a vulnerable 04WebServer, will create a fictitious log entry.

Example:

```
http://[hostname]/a%0a[22;45;24]%20%20(74,632)%20[%90%b3%8f%ed%82%c9%8f%49%97%b9%82%b5%82%dc%82%b5%82%bd]%20GET%20/hack
```

The log entries that are created are shown below. The fake entry is highlighted in red. Note that the : character is filtered and hence, cannot be created correctly in the logs.

```
[22:44:54] <10.0.0.4> (521,715) [ w . . . t @ C . . . . . ] GET /a  
[22;45;24] <192.168.1.3> (74,632) [ . . . I . . . . . ] GET /hack
```

3. Requesting COM2 or other DOS devices in the URL may prevent the Server from Restarting Properly

The attacker may specify the COM2 device in the request URL. This will cause the web server to open a handle to the device. Doing so will prevent the server from restarting properly the next time it needs to be restarted using servercontroller.exe or using Window's Service Control Manager. The following sample HTTP request demonstrates this. If using COM2 doesn't work on your test server, try other DOS devices like COM1, AUX, PRN, etc, until the server managed to "open" a DOS device.

Example:

```
http://[hostname]/COM2
```

Disclosure Timeline

30 Jul 04 – Vulnerabilites Discovered

30 Jul 04 – Initial Author Notification (no reply)

03 Aug 04 – Second Author Notification

04 Aug 04 – Author Reply (new version will be released by end August)

25 Oct 04 – Third Author Notification (no reply)

11 Nov 04 – Public ReleaseVulnerable Systems:

* 04WebServer version 1.42

04WebServer is a HTTP server developed by Soft3304 for Windows platforms. It is an easy-to-configure personal HTTP server that supports CGI, SSI, WebDAV and SSL/TLS. This advisory documents three vulnerabilities that were found in version 1.42 of 04WebServer. This includes a XSS vulnerability, lack of character filtering when writing to log file, and potential server restart problem after requesting a DOS device in the URL.

1. Cross-Site Scripting (XSS) Vulnerability in Default Error Page

When the user requests for a non-existing page from the web server, the default error page Response_default.html will be served out to user. This page displays the user's requested URL without properly escaping HTML special characters. This may be exploited by a malicious user to execute malicious Javascript on the victim's browser, stealing his cookie. The following sample HTTP request demonstrates the XSS vulnerability by displaying a harmless popup dialog box.

Example:

```
http://[hostname]/<script>alert('XSS');</script>
```

2. Lack of Character Filtering allows an Attacker to Inject Arbitrary Characters into Log File

User's HTTP requests are logged into a text file in the \04WebServer142\Logs directory. The server performs only minimally filtering on the request URL before writing it into the log file. This allows the attacker to inject arbitrary characters into the log file. In particular, it may be possible for the attacker to submit specifically crafted HTTP requests that would create fictions entries in the log. The following HTTP request, when submitted to a vulnerable 04WebServer, will create a fictions log entry.

Example:

```
http://[hostname]/a%0a[22;45;24]%20%20(74,632)%20[%90%b3%8f%ed%82%c9%8f%49%97%b9%82%b5%82%dc%82%b5%82%bd]%20GET%20/hack
```

The log entries that are created are shown below. The fake entry is highlighted in red. Note that the : character is filtered and hence, cannot be created correctly in the logs.

```
[22:44:54] <10.0.0.4> (521,715) [ w . . . . t @ C . . . . . ] GET /a  
[22:45:24] <192.168.1.3> (74,632) [ . . . I . . . . . ] GET /hack
```

3. Requesting COM2 or other DOS devices in the URL may prevent the Server from Restarting Properly

The attacker may specify the COM2 device in the request URL. This will cause the web server to open a handle to the device. Doing so will prevent the server from restarting properly the next time it needs to be restarted using servercontroller.exe or using Window's Service Control Manager. The following sample HTTP request demonstrates this. If using COM2 doesn't work on your test server, try other DOS devices like COM1, AUX, PRN, etc, until the server managed to "open" a DOS device.

Securiteam: [NT] 04WebServer Multiple Vulnerabilities (CSS, Log File Injection, AUX DoS)

Example:

http://[hostname]/COM2

Disclosure Timeline

- 30 Jul 04 – Vulnerabilities Discovered
- 30 Jul 04 – Initial Author Notification (no reply)
- 03 Aug 04 – Second Author Notification
- 04 Aug 04 – Author Reply (new version will be released by end August)
- 25 Oct 04 – Third Author Notification (no reply)
- 11 Nov 04 – Public Release

ADDITIONAL INFORMATION

The information has been provided by <mailto:jerome@athias.fr> JXrXme
ATHIAS.

The original article can be found at:

<<http://www.security.org.sg/vuln/04webserver142.html>>

<http://www.security.org.sg/vuln/04webserver142.html>

=====

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.