

[NT] WebSite Pro Vulnerable to Source Code Disclosure (8.3 Name Format)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0089.html>

From: support@securiteam.com

Date: 05/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 21 May 2002 22:55:00 +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.

WebSite Pro Vulnerable to Source Code Disclosure (8.3 Name Format)

SUMMARY

<<http://www.deerfield.com/>> WebSite Pro supports, as many other web servers, requests of files in their 8.3 format name. A vulnerability in the product allows it to be tricked (under certain configurations) to present an unparsed server side script.

DETAILS

Vulnerable systems:

- * Deerfield Website Pro 3.1.11.0 and prior

Immune systems:

- * Deerfield Website Pro 3.1.13.0

Background:

On Windows platforms, each "long file name" (file name that is not in DOS 8.3 format) has a "short file name" (in DOS 8.3 format) alternate name.

For example, "longfilename.txt" (which is not in DOS 8.3 format) has the alternate file name "longfi~1.txt", and "name.jumbo" has an alternate file name "name~1.jum". The short file name is formed by taking the name part of the file name (all characters up to the extension), trimming it to six

Securiteam: [NT] WebSite Pro Vulnerable to Source Code Disclosure (8.3 Name Format)

characters if necessary, and appending "~1" to it, and then trimming the extension to three characters if necessary. If there is already a file with that same (alternate) name in the directory, then the number (after the "~") is incremented until a free name is found. This scheme has one exception – if the name part is 1–2 characters long, then a different algorithm is used to produce the name part.

Technical details:

Web servers typically associate a handler to a resource according to its extension. Typically, when no handler is associated with a particular extension, a default handler is used (usually returning the raw file).

WebSite Pro, running on Windows platforms, fails to identify resources, which are requested in their alternate 8.3 format as such, and will simply try to serve these files in the standard manner. This means that the handler associated with the extension is invoked, and the file is served through this handler (other, non–vulnerable web servers refuse to serve files in the alternate 8.3 format). This has a severe security impact in the following configuration:

- A scripting extension name is 4 or more characters long (e.g. jhtml/jhtm and shtml/shtm).
- The trimmed extension (jht and sht) is not associated with the proper handler (usually, not associated with any handler).
- The requested script name (excluding the extension) is longer than two characters. For example: hello.jhtml and helloworld.shtml In such case, when requesting the alternate file name (for the script resource), e.g. hello~1.jht and hellow~1.sht, the vulnerable web server does not identify the resource name as an alternate name for a long file name, and attempts to serve the resource in the standard way. The server first extracts the extension ("jht" and "sht"), then associate a handler to it (since no handler is defined for "sht" or "jht" the default handler will be used in both cases), and invoke the handler, which returns the file as–is, without running it. This means that the script source is returned to the client, instead of the output of the script invocation.

Solution:

If you are running Deerfield WebSite Pro 3.1.11.0, upgrade to version 3.1.13.0, which is available at:

<<http://www.deerfield.com/download/website/>>

<http://www.deerfield.com/download/website/>

Workaround:

1. On NTFS (32–bit), you can disable the creation of the 8.3–compliant short file name for files with long file names by enabling (setting to 1) the "NtfsDisable8dot3NameCreation" registry key (registry path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\). However, this step may cause compatibility problems with 16–bit applications.

Securiteam: [NT] WebSite Pro Vulnerable to Source Code Disclosure (8.3 Name Format)

2. Associate the 8.3 format of the file extension with the same handler as the original file extension, e.g. if the extension in use is .jhtml, you should associate .jht with the same handler.

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.

-
- *Previous message:* support@securiteam.com: "[NEWS] Cisco IOS ICMP Redirect DoS"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)