

[NT] DOS Reserved Filenames Cause ColdFusion To Reveal Physical Web Root

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0052.html>

From: support@securiteam.com

Date: 05/11/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 11 May 2002 23:31:14 +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.

DOS Reserved Filenames Cause ColdFusion To Reveal Physical Web Root

SUMMARY

Certain DOS reserved filenames, such as NUL or PRN, can cause ColdFusion to display the path to the web root directory.

DETAILS

Affected Software Versions:

* ColdFusion Server for Windows 4.x, 5 (All Editions)

For example:

Error Diagnostic Information

Cannot open CFML file

The requested file "c:\inetpub\wwwroot\NUL.cfm" cannot be found.

When two or more periods are used in the filename, a different message is displayed:

Error Diagnostic Information

The template specification, 'c:\InetPub\wwwroot\NUL..cfm', is illegal.

Securiteam: [NT] DOS Reserved Filenames Cause ColdFusion To Reveal Physical Web Root

Information about the web root location does not by itself grant unauthorized access.

This information could potentially be useful in conjunction with some other vulnerability, especially if the web root has been changed from the default location: c:\inetpub\wwwroot.

Solutions:

Two solutions are available to prevent IIS from passing DOS reserved filenames to ColdFusion for processing.

- 1) Install and configure the Microsoft URLScan Security Tool.
- 2) Change IIS properties to check that files exist.

Method 1 – The Microsoft URLScan utility

The URLScan IIS Security Tool and instructions is available at:
<<http://www.microsoft.com/technet/security/tools/URLscan.asp>>
<http://www.microsoft.com/technet/security/tools/URLscan.asp>

To configure URLScan to prohibit DOS reserved filenames, add the following entries to the urlscan.ini file located in
C:\WINNT\system32\inetrv\urlscan.

```
[DenyUrlSequences]
/NUL. ; Don't allow DOS reserved filenames as valid files
/COM1.
/COM2.
/COM3.
/LPT1.
/LPT2.
/PRN.
/AUX.
```

Method 2 – IIS Check that file exists

In the IIS Properties dialog:

```
choose: Master Properties for [WWW Service]
select: [Edit]
select: [Home Directory] tab
select: [Configuration] button
find: Application Mappings for:
cfm C:\CFUSION\bin\iscf.dll ALL
select: [Edit]
enable: [Check that file exists] checkbox
select: [OK]
```

When prompted – apply this change to all virtual directories that can contain ColdFusion templates

Repeat this procedure to change the Application Mappings for: .dbm
C:\CFUSION\bin\iscf.dll ALL

Securiteam: [NT] DOS Reserved Filenames Cause ColdFusion To Reveal Physical Web Root

This second method may have two disadvantages:

- * The IIS error page will display for non-existent template, instead of the ColdFusion error page
- * CFGGRAPH cannot be used to create graphs as .jpg (JPEG) files

What Customers Should Do

Customers are advised to implement one of the two methods described if disclosure of the IIS web root is a security concern.

ADDITIONAL INFORMATION

The information has been provided by <mailto:benjamin@conceptis.com>
Benjamin Keller.

=====

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] mnoGoSearch Found To Be Vulnerable to a Heap Overflow"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)