

# [UNIX] TYPO3 Web Content Manager File System Path Disclosure

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00087.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 25 Jan 2006 09:46:19 +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>

-----

TYPO3 Web Content Manager File System Path Disclosure

---

## SUMMARY

TYPO3 is "a free Open Source content management system for enterprise purposes on the web and in Intranets. It offers full flexibility and extendability while featuring an accomplished set of ready-made interfaces, functions and modules".

The vulnerability discovered in TYPO3, allows remote users to disclose the file system path of the application when requesting certain files.

## DETAILS

Vulnerable Systems:

- \* TYPO3 version 3.7.1

The following files were found to disclose the application path:

<http://hostname/typo3/t3lib/thumbs.php>

<http://hostname/t3lib/showpic.php>

<http://hostname/t3lib/stdtdb/tables.php>

The issue is due to the application failing to properly determine its own

## [UNIX] TYPO3 Web Content Manager File System Path Disclosure

physical path and therefore trying to 'require()' a wrong class file.

Vulnerable code:

>From init.php, line 71:

```
define('PATH_thisScript',str_replace('/',',', str_replace('\\',',',
/php_sapi_name()=='cgi'||php_sapi_name()=='isapi'
||php_sapi_name()=='cgi-fcgi') && ($_SERVER['ORIG_PATH_TRANSLATED']?
$_SERVER['ORIG_PATH_TRANSLATED']:$_SERVER['PATH_TRANSLATED'])?
($_SERVER['ORIG_PATH_TRANSLATED']?
$_SERVER['ORIG_PATH_TRANSLATED']:$_SERVER['PATH_TRANSLATED']) :
($_SERVER['ORIG_SCRIPT_FILENAME']?$_SERVER['ORIG_SCRIPT_FILENAME'] :
$_SERVER['SCRIPT_FILENAME']));
```

>From the PHP manual:

"You can define a constant by using the define()-function. Once a constants defined, it can never be changed or undefined"

The vulnerable files listed above fail to include init.php and the

'PATH\_thisScript' variable is locally calculated:

```
define('PATH_thisScript',str_replace('/',',', str_replace('\\',',',
/php_sapi_name()=='cgi'||php_sapi_name()=='isapi'
||php_sapi_name()=='cgi-fcgi')&&($_SERVER['ORIG_PATH_TRANSLATED']?$_SERVER[
ORIG_PATH_TRANSLATED']:$_SERVER['PATH_TRANSLATED'])?
($_SERVER['ORIG_PATH_TRANSLATED']?$_SERVER['ORIG_PATH_TRANSLATED']:$_SERVER[
'PATH_TRANSLATED']):($_SERVER['ORIG_SCRIPT_FILENAME']?$_SERVER['ORIG_SCRIPT_
FILENAME']:$_SERVER['SCRIPT_FILENAME']));
```

```
define('PATH_site', ereg_replace('[^/]*.[^/]*$',",PATH_thisScript));
```

```
define('PATH_t3lib', PATH_site.'t3lib/'); define('PATH_tslib',
PATH_site.'tslib/');
```

At this point, constants 'PATH\_t3lib' and 'PATH\_tslib' contain wrong values and any 'require()' function using these constants will not work and will disclose the file system path.

Disclosure Timeline:

Contact was initially made via the TYPO3 bug reporting system on January 13th 2006.

Patch Availability:

On January 14th a patch for the issue was published on the site (

<<http://bugs.typo3.org/view.php?id=2248>>

<http://bugs.typo3.org/view.php?id=2248>)

### ADDITIONAL INFORMATION

The information has been provided by Rodrigo Marcos.

The original article can be found at:

<<http://www.irmplc.com/advisories.htm>>

[UNIX] TYPO3 Web Content Manager File System Path Disclosure

<http://www.irmpc.com/advisories.htm>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.

---

- Prev by Date: [\*\[REVS\] Security Testing Demystified\*](#)
- Next by Date: [\*\[REVS\] XST Strikes Back\*](#)
- Previous by thread: [\*\[REVS\] Security Testing Demystified\*](#)
- Next by thread: [\*\[REVS\] XST Strikes Back\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)