

# [UNIX] TikiWiki PHP Code Evaluation Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-11/msg00008.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 1 Nov 2007 17:53:10 +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>

-----

TikiWiki PHP Code Evaluation Vulnerability

---

## SUMMARY

TikiWiki 1.9.8.1 fixes a broken white-list check (CVE-2007-5423) that is supposed to protect against arbitrary PHP code injection in a call to `create_function()`. When Stefan analyzed the bugfix we discovered that while the reported bug in the white-list check is now repaired, it is still possible to execute arbitrary PHP code by only using the strings allowed in the white-list.

However since TikiWiki 1.9.8.1 the vulnerability can only be triggered if the 'sheet' feature of TikiWiki is activated in the configuration.

## DETAILS

Vulnerable Systems:

- \* TikiWiki version 1.9.8.1 and prior

Immune Systems:

- \* TikiWiki version 1.9.8.2

TikiWiki's `tiki-graph_formula.php` creates an anonymous function with PHP's `create_function()` to dynamically evaluate a mathematical function supplied

by the user through the 'f' URL parameter.

To protect against arbitrary PHP code execution the TikiWiki developers have combined a blacklist and white-list approach. On the one hand they have blacklisted three characters and on the other hand they only allow certain alphanumerical strings in the user input.

The three blacklisted characters are

- ` – Allows execution of shell commands
- ' – String delimiter
- " – String delimiter

The white-list of allowed alphanumerical string does only contain mathematical function names like: sin, cos, tan, pow, ...

When TikiWiki was audited by ShAnKaR he discovered that the white-list check was incorrectly implemented and it was therefore possible to execute any PHP function. This vulnerability is known as CVE-2007-5423 and was fixed with the TikiWiki 1.9.8.1 update.

Unfortunately the repaired white-list does not protect against arbitrary PHP code execution because PHP supports variable functions and variable variables.

```
$varname = 'othervar';  
$$varname = 4; // set $othervar to 4
```

```
$funcname = 'chr';  
$funcname(95); // call chr(95)
```

Because TikiWiki's blacklist does not protect against the '\$' character, the injected PHP formulas can use temporary variables like \$sin, \$cos, \$tan, ...

It is therefore obvious that the protection can be bypassed by filling the temporary variables with strings representing names of other functions. Because of TikiWiki's black- and white-list this is a little bit tricky but possible.

First of all it seems hard to get any string at all into one of our temporary variables because all allowed functions only return numbers. There are however two PHP features that help: array to string conversion and handling of unknown constants.

```
$sin=cosh; // cosh is an unknown constant.  
// PHP assumes the string 'cosh' as value
```

```
$sin[]=pi(); // Creates an array  
$sin=$sin.$sin; // Stringconcat of arrays. Array to string  
// conversion. Becomes 'ArrayArray'
```

## [UNIX] TikiWiki PHP Code Evaluation Vulnerability

Using these tricks in combination with the ++ Operator that also allows incrementing alphanumerical strings it is possible to for example call the chr() function like this.

```
$tan=pi()-pi(); // Get 0 into $tan
$sin=cosh; // Get the string 'cosh' into $sin
$min=$sin[$tan]; // Get 'c' into $min
$tan++; // Get 1 into $tan
$min.=$sin[$tan+$tan+$tan] // Append 'h' to 'c'
$min.=$sin[$tan]; // Append 'o' to 'ch'
$min++; // Increment 'cho' to 'chp'
$min++; // Increment 'chp' to 'chq'
$min++; // Increment 'chq' to 'chr'
$min($tan) // Call chr(1)
```

With access to the chr() function it is possible to create all kind of strings and therefore call any other function, which obviously leads to arbitrary PHP code execution.

### Disclosure Timeline:

- 14. October 2007 – Notified security@xxxxxxxxxxxxx, patch in CVS
- 25. October 2007 – TikiWiki developers released TikiWiki 1.9.8.2
- 26. October 2007 – TikiWiki developers released TikiWiki 1.9.8.3
- 29. October 2007 – Public Disclosure

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:stefan.esser@xxxxxxxxxxxxx>>  
Stefan Esser.

The original article can be found at:

<<http://www.sektioneins.de/advisories/SE-2007-01.txt>>  
<http://www.sektioneins.de/advisories/SE-2007-01.txt>

=====

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@xxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxx)

=====  
=====

### 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.