

# [UNIX] PHPProjekt (Remote) Include Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-10/msg00005.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 1 Oct 2006 09:34:47 +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>

-----

PHPProjekt (Remote) Include Vulnerabilities

---

## SUMMARY

"PHPProjekt is a modular application for the coordination of group activities and to share informations and document via Intranet and internet. Components of PHPProjekt: Group calendar, project management, time card system, file management, contact manager, mail client and 9 other modules ...(feature list). PHPProjekt supports many protocols like ldap, soap and webdav and is available for 36 languages and 7 databases."

While searching for applications that are vulnerable to a new class of vulnerabilities inside PHP applications we took a quick look into the current PHPProjekt source code and discovered that a (remote) include vulnerability had been (re)introduced.

By overwriting a variable with user input it is possible to inject and execute arbitrary PHP code. Overwriting this variable is possible regardless of the register\_globals setting.

## DETAILS

PHPProjekt includes several files from different paths. In earlier versions it was possible to overwrite the base path variable \$path\_pre from the

## [UNIX] PHProjekt (Remote) Include Vulnerabilities

outside and use it to include arbitrary files or URLs. This vulnerability had been fixed by checking the content of \$path\_pre and bailing out of the PHP script in case of an attack.

Unfortunately the code within PHProjekt was moved around, which resulted in \$lib\_path and \$lang\_path being filled before the request variables are extracted into the global namespace by the PHP script. (This globalisation is done by the code of PHProjekt and has nothing to do with PHP's register\_globals feature).

Because of this construction it is possible to include arbitrary PHP files by filling \$lib\_path or \$lang\_path through f.e. the URL.

This vulnerability was now fixed by modifying all include paths to use constants instead of variables, because constants cannot be overwritten once they are set.

### Disclosure Timeline:

- 21. September 2006 – Contacted PHProjekt developers by email
- 28. September 2006 – Updated PHProjekt was released
- 29. September 2006 – Public Disclosure

### Recommendation:

It is strongly recommended to upgrade to the newest version of PHProjekt 5.1.2 which you can download at:

<http://www.phprojekt.com/download/phprojekt.tar.gz>  
<http://www.phprojekt.com/download/phprojekt.tar.gz>

As usual we very strongly recommend to install our Suhosin PHP extension, because it is the only solution that stops all PHP remote URL includes. The often advertised allow\_url\_fopen configuration directive does NOT protect against 'php://input' or 'data:' URL types. Suhosin additionally can stop several directory traversal attacks that try to include local

### ADDITIONAL INFORMATION

The information has been provided by [sesser@xxxxxxxxxxxxxxxxxxxx](mailto:sesser@xxxxxxxxxxxxxxxxxxxx)  
Stefan Esser.

The original article can be found at:

[http://www.hardened-php.net/advisory\\_062006.129.html](http://www.hardened-php.net/advisory_062006.129.html)  
[http://www.hardened-php.net/advisory\\_062006.129.html](http://www.hardened-php.net/advisory_062006.129.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@xxxxxxxxxxxxxxxx

[UNIX] PHPProjekt (Remote) Include Vulnerabilities

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.