

[UNIX] phpAutoMembersArea File Inclusion

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-08/msg00023.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 6 Aug 2006 17:24:03 +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>

phpAutoMembersArea File Inclusion

SUMMARY

<<http://www.dwalker.co.uk/phpautomembersarea/>> phpAutoMembersArea (phpAMA) is a "PHP MySQL automated members area". A file inclusion vulnerability in phpAMA allows remote attackers to cause the product to execute arbitrary code.

DETAILS

Vulnerable Systems:

* phpAutoMembersArea version 3.2.5

Vulnerable code in auto_check_renewals.php (line 20):

```
....  
include($installed_config_file);  
....
```

As can be seen \$installed_config_file is not properly sanitized before being used.

Solution:

A patch for the mentioned vulnerability can be found at:

<<http://dwalker.co.uk/forum/viewtopic.php?t=517>>
<http://dwalker.co.uk/forum/viewtopic.php?t=517>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:webmaster@xxxxxxxxxxxxxxxx>>
Philipp Niedziela.
The original article can be found at:
<http://www.bb-pcsecurity.de/sicherheit_83.htm>
http://www.bb-pcsecurity.de/sicherheit_83.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.