

Securiteam: [UNIX] phpAdsNew Multiple Vulnerabilities (Path Disclosure, SQL Injection)

[UNIX] phpAdsNew Multiple Vulnerabilities (Path Disclosure, SQL Injection)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0062.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/15/05

To: list@securiteam.com

Date: 15 Nov 2005 16:19:37 +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>

phpAdsNew Multiple Vulnerabilities (Path Disclosure, SQL Injection)

SUMMARY

<<http://www.phpadsnew.com/>> phpAdsNew is "a banner management and tracking system written in PHP". Multiple security vulnerabilities in phpAdsNew allow remote attackers to disclose the true path under which the product was installed, and to cause the program to execute arbitrary SQL statements.

DETAILS

Vulnerable Systems:

* phpAdsNew version 2.0.6

Full Path Disclosure in create.php:

If user can access the misc/revisions/create.php, the script will echo the whole installation path to the user:

"Starting scan at /var/www/mysite/html/ads"

If the revision script completes successfully, the user can then try to access libraries/defaults/revisions.txt, which will then reveal all files and their revisions and hashes, thus furthermore revealing all files that

Securiteam: [UNIX] phpAdsNew Multiple Vulnerabilities (Path Disclosure, SQL Injection)

have been manually modified by the site admin.

The revisions.txt will also reveal any file that has been added under the installation tree, unless it's hidden (starts with '.')

Full Path Disclosures in the following files (Just by accessing with browser):

admin/lib-updates.inc.php
admin/lib-targetstats.inc.php
admin/lib-size.inc.php
admin/lib-misc-stats.inc.php
admin/lib-hourly-hosts.inc.php
admin/lib-hourly.inc.php
admin/lib-history.inc.php
admin/graph-daily.php

SQL-injection in logout.php / lib-sessions.inc.php:
phpAdsNew doesn't properly validate the sessionID it receives from cookie when it tries to log out the user. And it doesn't even check if the user is really logged in in the first place, thus allowing unauthorized users to feed data into the SQL-query that's supposed to clean the phpads_session-table. Take into note though that this requires magic_quotes_gpc to be off.

Impact:

A remote attacker could exploit this to learn installation paths on server, as well as to locate new files and possible manually modified files.

If magic_quotes_gpc is off, a remote attacker can also compromise the integrity of the database.

ADDITIONAL INFORMATION

The information has been provided by <mailto:toni.koivunen@fitsec.com>
Toni Koivunen.

The original article can be found at:
<<http://www.fitsec.com/advisories/FS-05-01.txt>>
<http://www.fitsec.com/advisories/FS-05-01.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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

Securiteam: [UNIX] phpAdsNew Multiple Vulnerabilities (Path Disclosure, SQL Injection)

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.